Manual Estratégico para la Comprensión, Detección y Respuesta ante Interferencias GPS en Operaciones Logísticas LATAM

Mtro. Mauricio Alan Illera Diaz

CVU: 2226610 / ORCID ID: 0009-0001-1505-4170 / SCOPUS ID: OSI-4768-2025 / SSRN: 9514252 / CTI: 490636 / CNPq: 5501442111063885 / CvLAC: 2495955

Manual Estratégico para la Comprensión, Detección y Respuesta ante Interferencias GPS en Operaciones Logísticas LATAM
Jamming, Spoofing y Resiliencia Operativa en Seguridad y Monitoreo

PRESENTACIÓN
Propósito del manual
Alcance operativo y estratégico
A quién está dirigido

- Centros de monitoreo
- Seguridad corporativa
- Operaciones logísticas
- Gestión de riesgos
- Inteligencia y análisis
- Liderazgo operativo

Objetivos generales
Metodología de comprensión estratégica
Del monitoreo reactivo a la resiliencia operacional

INTRODUCCIÓN GENERAL
La evolución de la amenaza en operaciones logísticas
1. Transformación del robo al transporte

- Del asalto físico a la invisibilidad operativa
- Profesionalización criminal
- Uso de tecnologías de interferencia

2. Dependencia tecnológica y vulnerabilidad

- El GPS como núcleo de la trazabilidad moderna
- Riesgos de depender de una sola fuente

3. La guerra electrónica aplicada al transporte

- Interferencia
- Manipulación
- Ocultamiento digital
- Negación de posicionamiento

4. El nuevo paradigma operativo

- La confianza en la información
- Resiliencia operacional
- Inteligencia aplicada a monitoreo

PARTE I — COMPRENDER
Módulo 1. Fundamentos GNSS y posicionamiento satelital
1.1 ¿Qué es realmente un GPS?

- Diferencia entre GPS y GNSS
- Principales constelaciones satelitales
- Conceptos básicos de posicionamiento

1.2 ¿Cómo funciona el posicionamiento satelital?

- Satélites
- Señales
- Tiempo y sincronización
- Trilateración

1.3 ¿Qué calcula realmente un receptor?

- Posición
- Velocidad
- Tiempo
- Precisión e incertidumbre

1.4 Arquitectura de un dispositivo GPS logístico

- Antena
- Receptor
- Firmware
- Módulo celular
- Sensores auxiliares

1.5 Del satélite al centro de monitoreo

- Flujo de datos
- Plataformas
- Telemetría
- Eventos y alertas

1.6 El GPS como evidencia operativa

- Trazabilidad
- Auditoría
- Validación de rutas
- Limitaciones del GPS como única verdad

Módulo 2. Vulnerabilidad y dependencia tecnológica

2.1 ¿Por qué el GPS es vulnerable?

- Debilidad natural de la señal
- Dependencia de radiofrecuencia
- Sensibilidad ambiental

2.2 Factores que afectan el posicionamiento

- Clima
- Infraestructura
- Urbanización
- Multipath
- Túneles y zonas de sombra

2.3 Vulnerabilidad vs inutilidad

- Comprender el riesgo real
- Riesgo operativo aceptable

2.4 Integridad de señal

- Confianza operacional

- Coherencia de datos
- Indicadores de autenticidad

Módulo 3. Taxonomía de amenazas GNSS y RF

3.1 Amenazas no intencionales

- Saturación RF
- Interferencia urbana
- Errores de infraestructura

3.2 Amenazas intencionales

- Jamming
- Spoofing
- Meaconing
- Repetidores ilegales
- Ataques híbridos

3.3 Amenazas internas

- Sabotaje
- Manipulación deliberada
- Desconexión operativa

3.4 Amenazas combinadas

- Bloqueo GNSS + inhibición celular
- Manipulación multisistema

3.5 Impacto operacional de las amenazas RF

- Pérdida de visibilidad
- Ruptura de trazabilidad
- Afectación de continuidad

PARTE II — DETECTAR

Módulo 4. Interferencia deliberada: Jamming

4.1 ¿Qué es un jammer?

- Definición
- Objetivo operacional

4.2 ¿Cómo funciona el jamming?

- Interferencia por ruido
- Saturación del receptor
- Bandas afectadas

4.3 Tipologías de jammer

- Portátiles
- Vehiculares
- Alta potencia
- Multi-banda

4.4 Impacto operativo del jamming

- Ceguera temporal
- Pérdida de monitoreo

- Ventanas de oportunidad criminal

4.5 Indicadores técnicos de jamming

- Pérdida abrupta GNSS
- Degradación de precisión
- Patrones RF

4.6 Indicadores operativos

- Corredores recurrentes
- Horarios críticos
- Conductas anómalas

4.7 Detección avanzada de interferencia

- Correlación multisensor
- Validación contextual
- Detección geoespacial

4.8 Respuesta operativa ante jamming

- Confirmación de evento
- Escalamiento
- Continuidad operativa
- Preservación de evidencia

Módulo 5. Manipulación de navegación: Spoofing

5.1 ¿Qué es el spoofing?

- Diferencia entre bloquear y engañar
- Alteración de posicionamiento

5.2 ¿Cómo funciona el spoofing?

- Señales falsas
- Suplantación de navegación

5.3 Impacto del spoofing en logística

- Rutas falsas
- Auditorías alteradas
- Manipulación de evidencia

5.4 Indicadores técnicos de spoofing

- Saltos imposibles
- Trayectorias irreales
- Inconsistencias temporales

5.5 Validación multisensor

- INS
- CAN Bus
- Odómetro
- Telefonía celular

5.6 Detección avanzada

- Coherencia física
- Análisis temporal
- Correlación dinámica

5.7 Respuesta operativa ante spoofing
- Suspensión de confianza GNSS
- Escalamiento táctico
- Protección de evidencia

Módulo 6. Doppler, autenticidad y coherencia física
6.1 ¿Qué es el efecto Doppler?
- Explicación aplicada al GPS

6.2 Doppler y posicionamiento
- Velocidad
- Sincronización
- Precisión

6.3 Doppler y autenticidad de señal
- Coherencia de movimiento
- Validación dinámica

6.4 Alteraciones Doppler bajo jamming
6.5 Alteraciones Doppler bajo spoofing
6.6 El Doppler como herramienta de inteligencia operacional

Módulo 7. Monitoreo inteligente y detección avanzada
7.1 Más allá del punto en el mapa
- Monitorear comportamiento

7.2 Correlación multisensor
- GPS
- INS
- CAN Bus
- LTE
- Sensores físicos
- Telemetría

7.3 Detección basada en patrones
- Corredores de riesgo
- Horarios
- Tipologías de carga
- Conductas recurrentes

7.4 Inteligencia geoespacial aplicada
- Heatmaps
- Geocercas dinámicas
- Análisis espacial

7.5 Inteligencia predictiva
- Probabilidad de interferencia
- Riesgo contextual

7.6 Gestión de falsos positivos
- Drift natural

- Multipath urbano
- Latencia celular
- Errores de plataforma

PARTE III — RESPONDER
Módulo 8. Respuesta táctica y continuidad operativa
8.1 Qué hacer antes del evento
- Diseño de rutas
- Evaluación de riesgo
- Planeación preventiva

8.2 Qué hacer durante el evento
- Confirmación
- Escalamiento
- Coordinación táctica

8.3 Qué hacer después del evento
- Investigación
- Retroalimentación
- Ajuste operativo

8.4 Continuidad operacional bajo degradación GNSS
8.5 Preservación de trazabilidad crítica

Módulo 9. Matriz de respuesta logística y de seguridad
9.1 Niveles de alerta
- Verde
- Amarillo
- Naranja
- Rojo

9.2 Criterios de activación
- Técnicos
- Operativos
- Contextuales

9.3 Roles y responsabilidades
- Monitoreo
- Seguridad
- Operaciones
- Inteligencia
- Liderazgo

9.4 Escalamiento operativo
9.5 Coordinación interáreas
9.6 Protocolos de crisis

PARTE IV — RESILIENCIA OPERACIONAL
Módulo 10. Arquitectura resiliente y contramedidas

10.1 GPS vulnerable, operación resiliente
- Cambio de paradigma

10.2 Arquitecturas resilientes
- Multi-constelación
- Multi-banda
- INS híbrido
- Dead reckoning

10.3 Tecnologías complementarias
- LTE fallback
- Satcom
- LoRa
- Edge analytics

10.4 Detección basada en inteligencia artificial
10.5 Estrategias de redundancia operacional

Módulo 11. Modelo de madurez operacional
11.1 Nivel 1 — Monitoreo reactivo
11.2 Nivel 2 — Gestión por alertas
11.3 Nivel 3 — Correlación multisensor
11.4 Nivel 4 — Inteligencia predictiva
11.5 Nivel 5 — Resiliencia adaptativa
11.6 Evaluación de madurez organizacional
11.7 Roadmap de evolución operativa

PARTE V — CRIMINOLOGÍA E INTELIGENCIA
Módulo 12. Criminología aplicada a interferencias GPS
12.1 El jammer como facilitador criminógeno
12.2 Conductas previas al robo
12.3 Modus operandi contemporáneo
12.4 Temporalidad y oportunidad criminal
12.5 Ocultamiento digital y desaparición operativa
12.6 Correlación entre interferencia y eventos delictivos
12.7 Perfil operativo de células criminales
12.8 Inteligencia táctica aplicada al transporte

Módulo 13. Inteligencia geoespacial y análisis de riesgo
13.1 Corredores de riesgo
13.2 Zonas RF hostiles
13.3 Geoint aplicada a logística
13.4 Mapas de calor
13.5 Patrones territoriales
13.6 Riesgo dinámico operacional
PARTE VI — EVIDENCIA, AUDITORÍA Y GOBERNANZA

Módulo 14. Evidencia digital y trazabilidad forense
14.1 GPS como evidencia
14.2 Integridad de registros
14.3 Cadena de custodia digital
14.4 Preservación de logs

PRESENTACIÓN

Propósito del manual

El presente manual tiene como finalidad desarrollar una comprensión estratégica, técnica y operativa de las interferencias que afectan los sistemas de posicionamiento satelital empleados en operaciones logísticas, con énfasis en fenómenos como el jamming, el spoofing, la degradación de señal y otras formas de negación o manipulación de la navegación. Su propósito central es proporcionar una base sólida para interpretar estas amenazas no como fallas aisladas, sino como eventos que pueden comprometer la continuidad operativa, la seguridad patrimonial, la trazabilidad y la calidad de la toma de decisiones.

Su propósito no es únicamente explicar conceptos tecnológicos de manera teórica. En realidad, este documento busca transformar la manera en que las organizaciones comprenden la seguridad logística, la confiabilidad de la información y la relación entre tecnología, operación y riesgo. En un entorno donde la visibilidad digital se ha convertido en un elemento crítico para coordinar rutas, validar entregas, reaccionar a incidentes y reconstruir eventos, comprender las debilidades del ecosistema GNSS es tan importante como conocer sus beneficios.

Durante años, gran parte de las operaciones de monitoreo fueron construidas sobre una premisa aparentemente simple: si el GPS indica una posición, entonces la unidad se encuentra en ese punto. Aunque esta lógica permitió operar durante mucho tiempo con esquemas funcionales de seguimiento, el contexto actual demuestra que ya no es suficiente. La información de posicionamiento puede verse afectada por interferencias deliberadas, condiciones ambientales, errores de infraestructura, fallas de dispositivo o manipulaciones diseñadas para generar una percepción falsa de normalidad.

En consecuencia, el reto moderno ya no consiste únicamente en recibir datos, sino en determinar si esos datos son auténticos, coherentes, consistentes con el contexto operativo y suficientemente confiables para actuar sobre ellos. La diferencia entre una operación segura y una operación vulnerable no depende solamente de contar con más alertas, sino de interpretar mejor la información y distinguir entre una anomalía normal, una falla técnica y una acción hostil.

Las operaciones logísticas modernas dependen profundamente de información digital para sostener la continuidad operativa, la supervisión remota y la toma de decisiones en tiempo real. Entre los datos más relevantes se encuentran los relacionados con:

- la ubicación y la trayectoria real o aparente de la unidad;
- la velocidad, las detenciones y los tiempos de permanencia;
- los tiempos de tránsito, las ventanas de entrega y el cumplimiento de ruta;
- las geocercas, los eventos de excepción y las alertas críticas;
- la telemetría, los sensores auxiliares y los registros operativos;

- la trazabilidad histórica y la evidencia utilizada para auditoría e investigación.

Cuando esa información es alterada, bloqueada, degradada o falsificada, el problema deja de ser únicamente tecnológico. Se convierte en un problema operativo porque limita la capacidad de monitorear y reaccionar; estratégico porque compromete decisiones críticas; financiero porque puede generar pérdidas directas e indirectas; legal porque afecta la validez de la evidencia; y de seguridad porque reduce la oportunidad de prevención y respuesta ante un incidente.
Este manual busca responder a esa nueva realidad mediante una visión integral que conecte tecnología, operación, seguridad, análisis e inteligencia. A lo largo de sus capítulos se desarrollará una lógica progresiva: comprender el fenómeno, reconocer sus manifestaciones, detectar señales de alerta, responder con criterio y fortalecer la resiliencia organizacional frente a amenazas que evolucionan constantemente.
A lo largo del documento se abordarán, entre otros, los siguientes ejes temáticos:

- el funcionamiento real de los sistemas GPS y GNSS;
- las vulnerabilidades inherentes al posicionamiento satelital;
- las modalidades de interferencia, negación y manipulación de señal;
- los indicadores técnicos y operativos para detectar anomalías;
- los criterios para interpretar comportamientos sospechosos según el contexto;
- las respuestas operativas ante escenarios de degradación o engaño;
- y los principios para construir resiliencia organizacional y continuidad operativa.

La intención es desarrollar criterio operativo y no únicamente dependencia tecnológica. Un sistema puede generar miles de datos, pero si la organización no sabe interpretarlos, validarlos ni contrastarlos con otras fuentes, seguirá siendo vulnerable ante escenarios complejos.
En última instancia, la verdadera seguridad no surge de observar un punto en un mapa. Surge de comprender si la información que observamos es auténtica, coherente, verificable y suficientemente confiable para sustentar una decisión.

Alcance operativo y estratégico

Este manual tiene un alcance multidisciplinario y transversal. No ha sido concebido exclusivamente para áreas técnicas ni únicamente para especialistas en telecomunicaciones, sino para todos los actores que participan en la cadena de decisión, supervisión, prevención, análisis y respuesta dentro de una operación logística moderna.
Su enfoque integra dimensiones operativas, de monitoreo, seguridad, análisis de riesgos, inteligencia, continuidad operativa, investigación, criminología aplicada y toma de decisiones estratégicas. Esta amplitud es necesaria porque las interferencias GNSS no impactan a un solo departamento; afectan simultáneamente la ejecución de rutas, la capacidad de reacción, la confiabilidad del monitoreo, la administración del riesgo y la gobernanza de la operación.

- operaciones y coordinación logística;
- monitoreo, supervisión y control de unidades;
- seguridad patrimonial y respuesta a incidentes;
- gestión de riesgos y continuidad del negocio;
- inteligencia, investigación y análisis geoespacial;
- liderazgo operativo y toma de decisiones estratégicas.

El documento aborda tanto la dimensión tecnológica de las interferencias GNSS como las consecuencias operativas y criminales derivadas de ellas. Esta doble perspectiva es esencial, ya que una misma anomalía puede tener una explicación técnica inocua o formar parte de una secuencia delictiva cuidadosamente planificada. La diferencia entre ambas depende del análisis del contexto, de la correlación de señales y del criterio del personal que interpreta el evento.
Por ello, el alcance del manual comprende los siguientes niveles de comprensión:

Comprensión técnica

Explicar de manera clara cómo funcionan los sistemas GNSS, qué variables condicionan su desempeño, cuáles son sus vulnerabilidades inherentes y de qué forma pueden ser degradados, negados o manipulados por factores ambientales, técnicos o intencionales. Esta comprensión es indispensable para evitar interpretaciones simplistas y para reconocer que la señal satelital, aunque valiosa, no es infalible.

Comprensión operativa

Interpretar cómo las alteraciones de señal afectan la continuidad logística, la trazabilidad de la carga, la coordinación entre áreas y la toma de decisiones en escenarios de presión e incertidumbre. La comprensión operativa conecta el fenómeno técnico con sus consecuencias reales en entregas, tiempos, validaciones, alertamientos, reacción táctica y continuidad del negocio.

Comprensión táctica

Desarrollar capacidades concretas de detección, análisis y respuesta frente a eventos de interferencia, de modo que el personal pueda distinguir señales tempranas de riesgo, validar hipótesis y actuar con rapidez sin depender exclusivamente de un solo indicador tecnológico. La comprensión táctica traduce el conocimiento en acciones verificables y oportunas.

Comprensión estratégica

Construir resiliencia organizacional mediante procesos, protocolos, inteligencia, arquitectura tecnológica y criterios de gobernanza que permitan sostener la operación incluso cuando la información sea parcial, degradada o incierta. La comprensión estratégica busca que la organización no dependa de una sola capa de visibilidad, sino de un sistema robusto de validación, redundancia y adaptación.

Comprensión criminológica

Entender cómo las organizaciones criminales utilizan tecnologías de interferencia como facilitadores del robo, el ocultamiento, la manipulación operativa y la reducción de la capacidad de respuesta institucional. Este nivel de comprensión permite relacionar patrones tecnológicos con conductas delictivas, temporalidades, territorios, ventanas de oportunidad y esquemas de profesionalización criminal.
Este manual reconoce que el problema ya no es exclusivamente perder señal. El verdadero problema es perder visibilidad confiable sobre la operación y, con ello, perder la capacidad de decidir con fundamento en un momento crítico.

A quién está dirigido

Este manual está dirigido a profesionales, equipos y organizaciones que participan de manera directa o indirecta en procesos de monitoreo, seguridad, trazabilidad, análisis de riesgo y continuidad logística. Su contenido ha sido diseñado para ser útil tanto para perfiles técnicos como para responsables operativos y directivos, con el fin de construir un lenguaje común que permita interpretar con mayor precisión las amenazas asociadas a las interferencias GNSS y sus efectos en la operación.

Más que un documento especializado para un solo perfil, este manual busca articular perspectivas complementarias. La interferencia GPS no es exclusivamente un problema de telecomunicaciones ni únicamente un asunto de seguridad patrimonial; es una condición de riesgo transversal que afecta la visibilidad operativa, la confiabilidad de la evidencia, la coordinación entre áreas y la capacidad de respuesta. Por ello, su lectura resulta valiosa para toda función que dependa de información de posicionamiento para decidir, reaccionar, investigar o prevenir.

Centros de monitoreo

Este apartado resulta especialmente relevante para operadores, supervisores y coordinadores responsables del seguimiento de unidades, la atención de alertas, el análisis de eventos, la gestión de incidentes y la continuidad operativa. En estos entornos, la primera interpretación de una anomalía suele producirse en tiempo real, por lo que la calidad del juicio inicial puede influir directamente en la oportunidad de la respuesta.

Para los centros de monitoreo, el manual permite reforzar una idea esencial: monitorear no significa únicamente observar posiciones en pantalla. Significa interpretar comportamientos, detectar inconsistencias, reconocer patrones atípicos y evaluar si la información disponible refleja una condición real o una alteración deliberada. Esta diferencia es crítica cuando una pérdida de señal, un salto de posición o una ruta incoherente pueden ser la primera manifestación de una amenaza mayor.

En ese sentido, el objetivo es ayudar a evolucionar del monitoreo pasivo hacia un análisis inteligente, contextual y orientado a la toma de decisiones. Un centro de monitoreo maduro no sólo reacciona a alertas; también valida, compara, jerarquiza y anticipa.

Seguridad corporativa

El contenido también está dirigido a responsables de protección de activos, prevención de pérdidas, seguridad patrimonial, seguridad logística, investigación y respuesta a incidentes. Para estas áreas, comprender una interferencia GNSS implica reconocer que una alteración tecnológica puede ser, al mismo tiempo, una táctica de ocultamiento, una señal de preparación delictiva o una condición que reduzca la capacidad institucional de reacción.

Desde la perspectiva de seguridad corporativa, la interferencia GPS debe entenderse como una amenaza híbrida: tecnológica por su medio de ejecución, operacional por sus efectos sobre la visibilidad y criminológica por su posible relación con conductas delictivas. Esta lectura integral permite evitar diagnósticos reduccionistas y favorece respuestas más proporcionadas y oportunas.

El personal de seguridad necesita desarrollar criterios para comprender cómo operan estas amenazas, qué buscan ocultar, qué ventanas de oportunidad generan y cómo identificar señales tempranas de riesgo antes de que se materialice un incidente mayor.

Operaciones logísticas

Este manual también es útil para gerencias logísticas, coordinación de transporte, planeación operativa, control de rutas y responsables de continuidad operacional. Para estas funciones, las alteraciones GNSS no constituyen únicamente una anomalía técnica: pueden traducirse en retrasos, incumplimientos, ruptura de trazabilidad, mala asignación de recursos, decisiones equivocadas y degradación general del desempeño operativo.

Su propósito en este ámbito es fortalecer la comprensión de cómo las alteraciones GNSS impactan entregas, tiempos de tránsito, trazabilidad, cumplimiento de ruta, productividad y continuidad del negocio. Una operación puede parecer estable desde la planeación, pero volverse frágil si depende de información cuya autenticidad no ha sido validada suficientemente.

Gestión de riesgos

Este manual también está dirigido a profesionales responsables de análisis de amenazas, matrices de riesgo, evaluación de vulnerabilidades, continuidad de negocio y resiliencia organizacional. Para estas funciones, las interferencias GNSS deben entenderse como un riesgo transversal que no sólo afecta la localización de una unidad, sino la estabilidad de todo el sistema de decisión que depende de esa información. Cuando una organización incorpora el posicionamiento satelital como insumo crítico de control, auditoría, seguridad y respuesta, cualquier degradación o manipulación de la señal deja de ser un incidente técnico aislado y se convierte en una exposición estratégica.

Desde la perspectiva de gestión de riesgos, el objetivo es comprender que las interferencias GNSS representan simultáneamente riesgos operativos, porque interrumpen la trazabilidad y reducen la visibilidad; riesgos financieros, porque pueden derivar en pérdidas de carga, retrasos, penalizaciones y costos de recuperación; riesgos reputacionales, porque afectan la percepción de confiabilidad del servicio; y riesgos estratégicos, porque debilitan la capacidad organizacional para decidir con precisión en entornos de presión. Una evaluación madura no debe limitarse a preguntar qué tan probable es una pérdida de señal, sino también qué tan vulnerable es la organización cuando esa pérdida ocurre, cuánto tiempo tarda en detectarla, qué tan bien puede validar información alternativa y qué tan preparada está para continuar operando bajo incertidumbre.

Inteligencia y análisis

Este manual resulta especialmente valioso para áreas responsables de análisis de patrones, correlación de eventos, geointeligencia, investigación, inteligencia táctica y análisis criminal. En estos entornos, la interferencia GPS no debe analizarse como un evento aislado ni como una simple anomalía técnica. Debe interpretarse dentro de un contexto territorial, temporal, operativo y conductual, ya que su verdadero significado depende de la relación que guarda con la ruta, el tipo de carga, la recurrencia del corredor, la temporalidad del evento, el historial de incidentes y la conducta observada de la unidad.

La inteligencia aplicada al monitoreo busca transformar datos dispersos en hipótesis operativas útiles. Esto implica identificar recurrencias, detectar zonas RF hostiles, diferenciar entre fallas ambientales y acciones deliberadas, correlacionar interferencias con otros indicadores y construir una lectura anticipatoria del riesgo. En términos prácticos, una organización con capacidad analítica no sólo observa que hubo una pérdida de señal; también se pregunta por qué ocurrió ahí, en ese

momento, con esa carga, bajo ese patrón de comportamiento y con qué posibles efectos posteriores. Esa lógica es la que permite pasar de la observación reactiva a la anticipación estratégica.

Liderazgo operativo

El documento está igualmente orientado a directores, gerencias, líderes regionales, responsables de seguridad y demás tomadores de decisiones que definen prioridades, asignan recursos y establecen el nivel de madurez de la operación. Para la alta dirección, comprender la problemática GNSS no significa dominar cada detalle técnico, sino entender cómo una amenaza sobre la señal puede escalar rápidamente hacia una afectación de servicio, una exposición financiera, una crisis de seguridad o una falla de gobernanza.

La alta dirección necesita reconocer que la resiliencia logística moderna no depende únicamente de contar con tecnología, sino de la capacidad organizacional para interpretar información incierta, establecer redundancias, decidir con criterios claros y coordinar respuestas interáreas bajo presión. En otras palabras, la verdadera fortaleza de una organización no radica sólo en recibir datos, sino en contar con estructuras de decisión capaces de mantener continuidad aun cuando esos datos sean parciales, degradados o potencialmente engañosos.

Objetivos generales

Los objetivos principales de este manual no se limitan a transmitir conceptos básicos sobre GPS o GNSS. Buscan desarrollar una comprensión aplicada que permita interpretar con profundidad las vulnerabilidades del posicionamiento satelital, reconocer la lógica de las amenazas contemporáneas y traducir ese conocimiento en mejores decisiones de prevención, detección, respuesta y resiliencia. Bajo esa lógica, los objetivos generales pueden entenderse del siguiente modo:

1. Comprender el funcionamiento real del GPS y los sistemas GNSS

El primer objetivo es desarrollar un conocimiento claro sobre posicionamiento satelital, transmisión de señal, sincronización temporal, cálculo de posición y trazabilidad operativa. Comprender cómo funciona realmente un sistema GNSS permite dejar atrás visiones simplistas y reconocer que la ubicación mostrada en una plataforma es el resultado de procesos físicos, matemáticos y electrónicos que pueden verse afectados por múltiples variables. Esta base técnica resulta indispensable para interpretar correctamente cualquier anomalía posterior.

2. Comprender las vulnerabilidades inherentes al sistema

El segundo objetivo consiste en identificar por qué las señales GNSS pueden degradarse, perderse, bloquearse o manipularse. Esto implica entender la debilidad natural de la señal en el receptor, su sensibilidad al entorno radioeléctrico, la posibilidad de interferencia intencional y la facilidad con la que algunos receptores pueden confiar en señales falsas si no existen mecanismos suficientes de validación. Comprender la vulnerabilidad no significa concluir que el GPS es inútil; significa reconocer sus límites reales para diseñar operaciones más robustas.

3. Entender las amenazas modernas de interferencia

El tercer objetivo es explicar cómo funcionan amenazas como el jamming, el spoofing, las interferencias híbridas y otros mecanismos de ocultamiento digital. La diferencia entre bloquear y

engañar es fundamental: mientras el jamming busca negar o degradar el servicio, el spoofing busca inducir confianza en una posición falsa. En el contexto logístico, ambos pueden servir para abrir ventanas de oportunidad criminal, obstaculizar auditorías, romper la trazabilidad y deteriorar la capacidad de respuesta si no se detectan con oportunidad.

4. Desarrollar capacidades de detección

El cuarto objetivo es fortalecer la capacidad de identificar anomalías, patrones sospechosos, inconsistencias operativas y señales tempranas de riesgo. Detectar no significa sólo observar que un dato salió del parámetro esperado; significa evaluar si el evento tiene coherencia física, si coincide con el comportamiento del vehículo, si existen otras fuentes que lo confirman y si el contexto indica una falla ordinaria o una posible acción deliberada. Este objetivo impulsa un monitoreo más inteligente, menos dependiente de alertas aisladas y más orientado al análisis contextual.

5. Mejorar la respuesta operativa

El quinto objetivo consiste en establecer criterios claros para validar eventos, escalar incidentes, preservar continuidad y reducir incertidumbre. Una buena respuesta operativa no depende únicamente de actuar rápido, sino de actuar con fundamento. En escenarios de interferencia, una reacción precipitada puede agravar el problema, mientras que una validación estructurada, un escalamiento oportuno y una coordinación interáreas adecuada pueden contener el impacto y conservar trazabilidad crítica para investigación posterior.

6. Construir resiliencia operacional

El sexto objetivo es promover operaciones menos dependientes de una sola fuente tecnológica y más capaces de mantener continuidad bajo degradación parcial de información. La resiliencia operacional implica redundancia, validación cruzada, entrenamiento, protocolos adaptativos y una arquitectura que permita seguir operando aun cuando el posicionamiento satelital pierda confiabilidad. No se trata de eliminar totalmente la vulnerabilidad, sino de reducir su impacto y acortar el tiempo de desorganización que produce.

7. Integrar inteligencia y análisis estratégico

El séptimo objetivo es transformar datos operativos en capacidades de prevención, anticipación y toma de decisiones estratégicas. Esto supone aprender a convertir eventos aparentemente dispersos en patrones de riesgo, construir conocimiento sobre corredores críticos, reconocer tipologías de interferencia y alimentar procesos de mejora continua. Una organización madura no sólo responde a lo que ya ocurrió; aprende de cada evento para reducir exposición futura.

Metodología de comprensión estratégica

Este manual adopta una metodología basada en comprensión integral y no únicamente en repetición de protocolos. La razón es simple: las interferencias GNSS no siempre se manifiestan de manera evidente, continua o inequívoca. Pueden durar segundos, aparecer de forma intermitente, confundirse con fallas normales del entorno radioeléctrico o formar parte de estrategias criminales más amplias. Por ello, una metodología centrada sólo en respuestas automáticas resulta insuficiente para interpretar fenómenos complejos.

Tradicionalmente, muchas organizaciones han abordado la seguridad logística desde modelos reactivos: aparece una alerta, se ejecuta un procedimiento y se escala un evento. Aunque este enfoque ofrece cierta disciplina operativa, también presenta una limitación relevante: parte del supuesto de que la amenaza siempre será visible, inequívoca y compatible con reglas predefinidas. En la práctica, los eventos de jamming y spoofing pueden romper ese supuesto, porque degradan la información precisamente en el momento en que más se necesita validar la realidad del evento. Las amenazas actuales son más complejas porque operan sobre la confianza, no sólo sobre la señal. Una interferencia puede intentar negar servicio, engañar al receptor, generar ruido suficiente para ocultar una maniobra o simplemente sembrar incertidumbre para retrasar la reacción. Por ello, este manual propone una metodología basada en cinco niveles de comprensión que permiten interpretar el fenómeno desde distintos ángulos complementarios y construir una lectura más robusta del riesgo.

1. Comprender el fenómeno técnico

Antes de reaccionar, es necesario entender qué ocurre físicamente, cómo opera la señal y qué puede alterarla. Este nivel busca que el lector comprenda la base técnica del problema: la debilidad natural de la señal GNSS al llegar al receptor, la relevancia del tiempo y la sincronización, la sensibilidad a interferencias y la diferencia entre una pérdida legítima de cobertura y una alteración inducida. Sin este nivel de comprensión, cualquier análisis posterior corre el riesgo de apoyarse en interpretaciones superficiales.

2. Comprender el impacto operativo

Toda alteración tecnológica tiene consecuencias operativas. Una pérdida de integridad en la señal puede traducirse en ruptura de trazabilidad, incertidumbre en la ubicación, retrasos, exposición al riesgo, degradación de la coordinación y deterioro de la calidad de las decisiones. Este nivel metodológico conecta el fenómeno técnico con el negocio real: entregas que no se validan, rutas que no se interpretan correctamente, alertas que pierden confiabilidad y equipos que operan con menor certeza situacional.

3. Comprender el contexto

No toda pérdida GPS implica un delito y no toda anomalía implica un ataque. La interpretación correcta exige considerar ubicación, horarios, comportamiento histórico, contexto territorial, exposición del corredor, tipo de carga y correlación multisensor. Este nivel es fundamental porque permite discriminar entre un falso positivo, una falla normal del entorno, una degradación accidental y una acción deliberada. En otras palabras, el contexto es lo que convierte un dato aislado en una hipótesis significativa.

4. Comprender el comportamiento criminal

Las organizaciones criminales modernas pueden utilizar tecnología, inteligencia, análisis de vulnerabilidades y ocultamiento digital para aumentar la probabilidad de éxito de un evento. Comprender este nivel significa reconocer que algunas interferencias no buscan únicamente producir un fallo, sino facilitar una secuencia mayor de acciones: aproximación, desvío, inmovilización, transbordo, desaparición temporal o manipulación de evidencia. Leer la

interferencia como posible parte de un modus operandi es clave para anticiparse y no reaccionar demasiado tarde.

5. Comprender la resiliencia

La resiliencia no consiste en evitar completamente las fallas, sino en mantener capacidad operativa aun bajo degradación o incertidumbre. Este nivel de comprensión busca que la organización construya redundancias técnicas, protocolos adaptativos, capacidades humanas de validación y una cultura de decisión basada en evidencia múltiple. Una operación resiliente acepta que el entorno es imperfecto, pero no permite que esa imperfección paralice su capacidad de actuar.

Del monitoreo reactivo a la resiliencia operacional

Durante muchos años, el monitoreo logístico fue construido bajo un modelo esencialmente reactivo. El operador observaba posiciones, rutas, alertas, aperturas, desvíos y pérdidas de señal; cuando aparecía una anomalía, se reaccionaba. Este modelo fue funcional en un contexto donde muchas amenazas eran más visibles y lineales. Sin embargo, el entorno actual ha transformado radicalmente esa lógica, porque los actores hostiles comprenden cada vez mejor cómo funcionan los dispositivos, las plataformas, las geocercas y los protocolos de reacción.

Hoy, en muchos escenarios, ya no se busca únicamente intervenir una unidad en el plano físico. También se busca degradar la capacidad de la organización para verla, interpretarla y ubicarla correctamente. En ese sentido, la amenaza puede iniciar antes del robo físico, cuando la empresa pierde capacidad de confiar en la información que recibe. Ese cambio es crítico: el problema ya no es solamente la desaparición del vehículo, sino la pérdida anticipada de visibilidad confiable sobre lo que está ocurriendo.

Por ello, las organizaciones modernas deben evolucionar hacia modelos de resiliencia operacional. La resiliencia implica detectar incertidumbre, validar información, correlacionar fuentes, mantener continuidad y adaptarse rápidamente a escenarios degradados. El objetivo ya no es únicamente monitorear; el objetivo es conservar conciencia situacional aun cuando la información sea incompleta, alterada o incierta. En la práctica, esto exige combinar tecnología con criterio humano, procesos con inteligencia, y plataformas de monitoreo con capacidades de validación contextual.

INTRODUCCIÓN GENERAL

La evolución de la amenaza en operaciones logísticas

Las operaciones logísticas modernas dependen profundamente de tecnología digital para sostener visibilidad, control, trazabilidad, seguridad y continuidad operacional. Sin embargo, esa misma dependencia ha creado nuevas superficies de vulnerabilidad. A medida que el ecosistema logístico se volvió más conectado, también se volvió más sensible a la degradación de los datos que utiliza para decidir. En ese contexto, las interferencias GNSS han adquirido especial relevancia porque afectan una de las capas más críticas del sistema: la confianza en la ubicación, en la ruta, en el tiempo y en la evidencia operativa que sustenta la supervisión.

Durante años, el robo al transporte se caracterizó principalmente por violencia física, interceptación directa, bloqueos carreteros y control territorial. Hoy, el escenario ha evolucionado. Muchas organizaciones criminales ya no sólo buscan controlar físicamente una unidad; también buscan controlar, degradar o manipular la información relacionada con ella. Esta transición ha dado origen

a nuevas formas de ocultamiento operacional, entre las que destacan la interferencia de señal, la manipulación del posicionamiento, la desaparición digital temporal, la degradación del monitoreo y la falsificación de trazabilidad.
La amenaza actual combina crimen tradicional, tecnología accesible, inteligencia operativa y formas de guerra electrónica de bajo costo. Este fenómeno no es exclusivo de un solo sector ni de un solo país; distintos análisis recientes sobre transporte y seguridad han subrayado que el aumento de jamming y spoofing está obligando a replantear la forma en que se protege la navegación, la logística y la continuidad de operaciones críticas. Comprender esta evolución no es un ejercicio académico: es una condición necesaria para construir operaciones más resilientes, menos dependientes de una sola fuente de verdad y más preparadas para actuar bajo incertidumbre.

1. Transformación del robo al transporte

Del asalto físico a la invisibilidad operativa

Históricamente, el robo al transporte dependía sobre todo de la capacidad física para interceptar una unidad, someter al operador, controlar la carga y retirarse antes de que la organización reaccionara. En ese modelo tradicional, el éxito criminal estaba asociado principalmente a la fuerza, la rapidez, el conocimiento del terreno y la posibilidad de imponer control directo sobre el vehículo y su entorno inmediato. El centro del evento era físico: detener, dominar y desplazar.
La incorporación masiva de sistemas GPS y plataformas de monitoreo transformó profundamente ese escenario. La trazabilidad satelital permitió localizar unidades, detectar desvíos, reconstruir rutas, validar ventanas de entrega y responder con mayor rapidez ante eventos anómalos. Como consecuencia, muchas estructuras criminales comenzaron a adaptar sus métodos y entendieron que, para ejecutar con éxito un robo o un desvío de carga, ya no bastaba con controlar el vehículo en el plano físico: era necesario neutralizar primero la visibilidad digital que la organización tenía sobre él.
En ese nuevo contexto, el objetivo criminal dejó de ser únicamente robar; pasó a ser desaparecer operacionalmente durante el tiempo suficiente para impedir la reacción, romper la trazabilidad y ganar una ventana crítica de maniobra. Por ello, en muchos casos contemporáneos, la pérdida de señal ya no debe interpretarse como una consecuencia secundaria del evento, sino como una parte inicial del mismo, diseñada para degradar la conciencia situacional de la empresa antes de que ésta pueda actuar con fundamento.

Profesionalización criminal

Las estructuras criminales contemporáneas muestran niveles crecientes de organización, inteligencia, planeación, segmentación operativa y conocimiento tecnológico. En numerosos casos, los grupos estudian rutas, identifican horarios vulnerables, analizan patrones de monitoreo, estiman tiempos de reacción y reconocen debilidades tecnológicas de dispositivos, plataformas o protocolos. Esto significa que las organizaciones ya no enfrentan únicamente delincuencia oportunista, sino operaciones técnicamente adaptativas que aprenden, prueban, corrigen y evolucionan. Entender esta profesionalización es fundamental, porque obliga a sustituir respuestas genéricas por esquemas de seguridad basados en inteligencia, análisis de comportamiento y resiliencia operativa.

Uso de tecnologías de interferencia

La disponibilidad de dispositivos de interferencia ha aumentado y, con ello, también la capacidad de degradar el posicionamiento, inhibir comunicaciones o alterar información de navegación mediante herramientas relativamente accesibles. Jammers portátiles, inhibidores multibanda, repetidores ilegales, mecanismos de spoofing y configuraciones híbridas pueden modificar por completo la dinámica del monitoreo tradicional, porque ya no sólo se ataca el vehículo o la carga: se ataca la confianza de la organización en la información que recibe. Esta evolución explica por qué el monitoreo basado exclusivamente en una señal o en una sola fuente de datos resulta cada vez más insuficiente frente a amenazas contemporáneas.

2. Dependencia tecnológica y vulnerabilidad

El GPS como núcleo de la trazabilidad moderna

Riesgos de depender de una sola fuente

Uno de los principales problemas operativos modernos es la dependencia excesiva de una única fuente de verdad. Cuando una organización asume que si el GPS lo muestra entonces necesariamente es real, aparece una vulnerabilidad estructural. Ningún sistema aislado debe considerarse infalible. Toda información requiere validación, correlación, coherencia física y contexto. Las organizaciones resilientes no dependen únicamente del posicionamiento satelital; integran telemetría, sensores, análisis conductual, telefonía, odómetros, CAN Bus y otras fuentes capaces de confirmar o cuestionar la narrativa que ofrece la señal principal. La resiliencia comienza precisamente donde termina la confianza ciega.

3. La guerra electrónica aplicada al transporte

La guerra electrónica consiste, en términos generales, en utilizar el espectro electromagnético para interferir, degradar, negar, manipular o explotar sistemas electrónicos que dependen de señales de radiofrecuencia. Aunque durante mucho tiempo este concepto fue asociado principalmente al ámbito militar, hoy sus principios tienen implicaciones claras en entornos logísticos, criminales y de seguridad privada. En el transporte moderno, la guerra electrónica de bajo costo se manifiesta cuando una señal esencial para ubicar, sincronizar o comunicar una operación es afectada deliberadamente para reducir la capacidad de observación y reacción de la organización.

Interferencia

La interferencia consiste en introducir señales o ruido que dificultan o impiden la recepción legítima de las transmisiones satelitales. En logística, esto suele expresarse como pérdida repentina de GPS, degradación de precisión, caídas de señal aparentemente injustificadas o ausencia de comunicación en momentos críticos. Aunque a simple vista puede parecer una simple falla técnica, su efecto real es mucho más profundo: rompe la continuidad de la observación y crea una zona temporal de incertidumbre que puede ser explotada para desvíos, inmovilizaciones o movimientos no autorizados.

Manipulación

La manipulación implica alterar deliberadamente la información percibida por un sistema para que éste construya una interpretación falsa de la realidad. En el caso del spoofing, el receptor puede creer que se encuentra en una ubicación aparente válida, aunque esa posición no corresponda al

movimiento real de la unidad. Esta modalidad es especialmente delicada porque no siempre genera una ausencia visible de datos; por el contrario, puede mantener una apariencia de normalidad mientras desvía la confianza operativa hacia una narrativa falsa. Precisamente por ello, la manipulación es más difícil de detectar que la simple negación de servicio.

Ocultamiento digital

El ocultamiento digital no siempre busca destruir información ni apagar totalmente un dispositivo. En muchos casos, el objetivo consiste en volver invisible una operación durante un periodo crítico para mover unidades, alterar rutas, realizar transbordos o ejecutar un robo con menor probabilidad de reacción inmediata. Esta invisibilidad temporal puede ser suficiente para romper la continuidad del seguimiento y dificultar la reconstrucción posterior de los hechos. Por ello, una desaparición digital breve puede tener consecuencias operativas desproporcionadas frente a su duración aparente.

Negación de posicionamiento

La negación de posicionamiento consiste en impedir que la organización mantenga una conciencia situacional confiable. Cuando una empresa pierde visibilidad sobre una unidad, no sólo pierde un dato de ubicación: pierde capacidad de decisión, capacidad de reacción y certeza sobre la secuencia real del evento. La incertidumbre resultante puede retrasar escalamientos, generar hipótesis equivocadas y ampliar el margen de acción del adversario. Desde una perspectiva estratégica, negar posicionamiento equivale a degradar la capacidad de gobernar la operación en tiempo real.

4. El nuevo paradigma operativo

La confianza en la información

El verdadero centro del problema moderno ya no es únicamente el dispositivo GPS en sí mismo, sino la confianza que la organización deposita en la información que recibe. Toda operación depende de datos para decidir, escalar, validar entregas, reasignar recursos y reaccionar ante anomalías. Cuando esa información puede alterarse, degradarse o falsificarse, la organización necesita mecanismos de validación más avanzados que le permitan distinguir entre dato disponible y dato confiable. En otras palabras, el reto contemporáneo no es sólo recibir información, sino saber cuándo creerle y cuándo cuestionarla.

Resiliencia operacional

La resiliencia operacional consiste en mantener capacidad funcional aun bajo condiciones adversas, degradación parcial o incertidumbre informativa. Una operación resiliente detecta anomalías, valida información, adapta procesos y continúa operando sin paralizarse ante la pérdida de una sola fuente tecnológica. La resiliencia no elimina la amenaza, pero reduce su impacto, acorta el tiempo de desorganización y preserva la capacidad de actuar con criterio. Desde esta perspectiva, una organización madura no pregunta únicamente cómo evitar una interferencia, sino también cómo seguir gobernando la operación cuando la interferencia ocurra.

Inteligencia aplicada a monitoreo

El monitoreo moderno ya no puede limitarse a observar puntos en un mapa. Debe evolucionar hacia análisis conductual, correlación multisensor, inteligencia geoespacial, análisis predictivo y comprensión contextual. La verdadera ventaja operativa ya no está únicamente en tener

información, sino en comprenderla correctamente antes que los demás, detectar patrones débiles antes de que escalen y convertir datos dispersos en decisiones útiles. En un entorno donde la señal puede ser manipulada o negada, la inteligencia aplicada al monitoreo se convierte en una función crítica de anticipación, validación y protección operacional.

PARTE I — COMPRENDER

Módulo 1. Fundamentos GNSS y posicionamiento satelital

1.1 ¿Qué es realmente un GPS?

Cuando se habla de rastreo vehicular, monitoreo logístico o trazabilidad operativa, es común que el término "GPS" se utilice como una etiqueta genérica para cualquier sistema de ubicación satelital. Sin embargo, desde una perspectiva técnica, esa simplificación puede conducir a errores de interpretación importantes. GPS no equivale a toda la navegación satelital; en realidad, es sólo uno de los sistemas que integran el universo GNSS. Comprender esta diferencia resulta esencial porque muchas decisiones operativas, diagnósticos de falla y evaluaciones de riesgo dependen de saber con precisión qué tecnología está generando la posición, bajo qué principios funciona y cuáles son sus verdaderos límites.

Diferencia entre GPS y GNSS

¿Qué significa GPS?

GPS significa *Global Positioning System*. Se trata de un sistema de posicionamiento satelital desarrollado originalmente por el Departamento de Defensa de los Estados Unidos y posteriormente abierto a usos civiles y comerciales a escala global. Su función principal es permitir que un receptor determine variables como posición, velocidad, dirección y tiempo a partir de señales emitidas por satélites en órbita media terrestre. Aunque el nombre se ha vuelto sinónimo de localización en el lenguaje cotidiano, en términos técnicos el GPS representa una constelación específica y no la totalidad de las capacidades globales de navegación satelital.

¿Qué significa GNSS?

GNSS significa *Global Navigation Satellite System* y es el término genérico que engloba todos los sistemas de navegación satelital capaces de proporcionar servicios de posición, navegación y tiempo a escala global o regional. En otras palabras, el GPS es un tipo de GNSS, pero GNSS no significa únicamente GPS. Esta distinción es clave porque los receptores modernos suelen operar de forma multiconstelación, combinando señales de diferentes sistemas para mejorar precisión, disponibilidad, estabilidad y resiliencia frente a obstrucciones parciales o degradaciones de señal.

Principales constelaciones satelitales

Actualmente, el ecosistema GNSS está compuesto principalmente por cuatro constelaciones globales: GPS, operado por Estados Unidos; GLONASS, desarrollado por Rusia; Galileo, impulsado por la Unión Europea con un fuerte enfoque civil; y BeiDou, operado por China y con creciente presencia global. A estas se suman sistemas regionales como NavIC, en India, y QZSS, en Japón, que complementan la cobertura en zonas específicas. En la práctica, los receptores modernos de uso logístico ya no dependen de una sola constelación, sino que combinan varias al mismo tiempo. Esta arquitectura multi-GNSS incrementa el número de satélites visibles, mejora la

geometría de observación, fortalece la continuidad operativa en entornos urbanos complejos y reduce parcialmente la vulnerabilidad asociada a depender de una sola fuente de posicionamiento.

Conceptos básicos de posicionamiento

Para comprender cómo funciona el posicionamiento satelital, es necesario desmontar algunas ideas equivocadas muy extendidas. Un receptor GNSS no "ve" el mapa ni obtiene su ubicación desde internet; lo que hace es recibir señales de varios satélites, medir con enorme precisión el tiempo de viaje de esas señales y calcular matemáticamente una posición estimada. El mapa es sólo una representación visual posterior, mientras que la conexión celular sirve principalmente para transmitir los datos a una plataforma, no para producir el cálculo primario de ubicación. En el centro de este proceso se encuentra el tiempo: los satélites transmiten referencias temporales extremadamente precisas y el receptor, al estimar cuánto tardó cada señal en llegar, infiere distancias y luego posición. Esta lógica explica también por qué la señal GNSS es intrínsecamente vulnerable: viaja miles de kilómetros, llega muy debilitada al receptor y puede verse afectada por obstrucciones, reflexiones, ruido electromagnético o interferencia deliberada.

1.2 ¿Cómo funciona el posicionamiento satelital?

Para comprender cómo puede degradarse, bloquearse o manipularse un sistema GNSS, primero es indispensable entender cómo funciona en condiciones normales. El posicionamiento satelital es, esencialmente, un problema de tiempo, distancia, geometría y radiofrecuencia. No se trata de un "rastreador inteligente" que sabe por sí mismo dónde está, sino de un sistema de cálculo que combina señales sincronizadas, medición de tiempo de vuelo y geometría espacial para estimar posición, velocidad y tiempo. Esta base técnica es fundamental porque toda alteración posterior —ya sea accidental o deliberada— afecta precisamente alguno de esos componentes esenciales.
Los sistemas GNSS están formados por constelaciones de satélites que orbitan la Tierra y transmiten continuamente señales de radiofrecuencia con información temporal y orbital. El satélite no rastrea vehículos ni "sabe" dónde está el usuario; simplemente emite señales extremadamente precisas. El receptor, al escuchar simultáneamente varios satélites, calcula cuánto tardó cada señal en llegar. Dado que esas señales viajan a la velocidad de la luz, diferencias mínimas de tiempo implican diferencias medibles de distancia. Con esas distancias estimadas, el receptor aplica trilateración para determinar su posición. En términos prácticos, cuatro satélites constituyen el mínimo para resolver con confiabilidad latitud, longitud, altitud y error de reloj del receptor, aunque en la operación real disponer de más satélites mejora la geometría, reduce incertidumbre y fortalece la estabilidad del cálculo. Todo este proceso depende de una sincronización temporal extremadamente precisa, razón por la cual los satélites incorporan relojes atómicos y el sistema completo es altamente sensible a errores de tiempo, multipath, obstrucciones e interferencia RF.

1.3 ¿Qué calcula realmente un receptor?

Un receptor GNSS no calcula solamente una coordenada en el mapa. En realidad, genera un conjunto de variables críticas para la operación: posición, velocidad, tiempo y estimaciones de precisión o incertidumbre. La posición expresa la localización espacial estimada del equipo; la velocidad puede derivarse tanto del cambio de posición como del comportamiento Doppler de la señal; y el tiempo constituye una referencia central para ordenar eventos, auditar secuencias y

correlacionar información entre sistemas. Ninguno de estos valores debe interpretarse como certeza absoluta. Todo cálculo GNSS contiene márgenes de error condicionados por la calidad del receptor, la geometría satelital, el entorno urbano, el multipath, el estado de la antena, la interferencia y la calidad del firmware. Por ello, en operaciones logísticas maduras, la información GNSS debe leerse siempre junto con su contexto físico y operativo, no como una verdad aislada e incuestionable.

1.4 Arquitectura de un dispositivo GPS logístico

Un dispositivo GPS logístico no debe entenderse como una pieza única, sino como un pequeño ecosistema tecnológico donde varios componentes trabajan de forma coordinada. La antena recibe señales satelitales y su instalación influye directamente en sensibilidad, estabilidad y exposición al multipath. El receptor o chipset GNSS interpreta las señales, ejecuta los cálculos de posición y sincronización y determina la calidad del desempeño frente al ruido o a la degradación de señal. El firmware gobierna la lógica interna del dispositivo, el manejo de eventos y la forma en que se procesan y reportan los datos; si es deficiente, puede generar falsas pérdidas, errores o inconsistencias. A esto se suma el módulo celular, que normalmente transmite la información hacia la plataforma de monitoreo, y los sensores auxiliares —como acelerómetros, giroscopios, CAN Bus, odómetro o señales de ignición— que permiten validar comportamiento y enriquecer la capacidad de correlación. En conjunto, esta arquitectura explica por qué una falla operativa puede no originarse exclusivamente en el satélite o en la señal, sino en cualquiera de las capas que intervienen entre la recepción y la visualización del dato.

1.5 Del satélite al centro de monitoreo

Una de las ideas más equivocadas en el entorno logístico es pensar que el GPS “manda” directamente su información a la plataforma. En realidad, entre el satélite y el operador existe una cadena tecnológica compuesta por varias etapas: recepción satelital, cálculo de posición, generación de eventos, transmisión por red, procesamiento en servidor, interpretación de plataforma y visualización humana. Cada una de esas capas puede introducir retrasos, pérdidas, errores o vulnerabilidades. La plataforma sólo muestra lo que recibe y cómo lo interpreta; por tanto, si el dato original llega degradado, incompleto o manipulado, la visualización también quedará comprometida. Aquí la telemetría adquiere valor estratégico, porque aporta variables complementarias —como ignición, velocidad, aperturas, combustible, frenados o comportamiento vehicular— que permiten contrastar la narrativa GNSS. Del mismo modo, los eventos y alertas automáticas deben entenderse como señales de atención y no como pruebas concluyentes por sí mismas: su significado real depende del contexto, de la correlación con otras fuentes y de la capacidad analítica del centro de monitoreo.

1.6 El GPS como evidencia operativa

En la logística moderna, el GPS se ha convertido en una fuente central de evidencia operativa porque permite reconstruir rutas, tiempos, trayectorias y comportamientos asociados a una unidad o a una carga. Esta capacidad lo vuelve especialmente útil para auditorías, investigaciones, validación de cumplimiento, revisión de desvíos y reconstrucción de incidentes. Sin embargo, su valor probatorio depende de una condición crítica: la integridad del dato. Una ruta visualmente coherente no garantiza por sí sola autenticidad absoluta, del mismo modo que una secuencia ordenada en

plataforma no necesariamente refleja la realidad física sin distorsión. El error más peligroso consiste en asumir que todo lo visible en el sistema ocurrió exactamente como se presenta. En entornos donde puede existir degradación, bloqueo, manipulación o falsificación, el GPS debe ser tratado como evidencia valiosa pero no autosuficiente. Su mayor fuerza aparece cuando se integra con telemetría, contexto operativo, coherencia temporal y validación multisensor. En otras palabras, la evidencia GNSS no debe interpretarse como una única verdad, sino como una capa crítica dentro de un sistema más amplio de verificación operacional.

Módulo 2. Vulnerabilidad y dependencia tecnológica

La tecnología GNSS transformó radicalmente la logística moderna al permitir trazabilidad en tiempo real, supervisión remota, optimización de rutas, control operativo y capacidad de respuesta más rápida frente a eventos anómalos. Sin embargo, junto con esos beneficios surgió una realidad crítica: el posicionamiento satelital es inherentemente vulnerable. Comprender esa vulnerabilidad es indispensable porque una de las fallas más comunes en seguridad logística consiste en confundir disponibilidad tecnológica con invulnerabilidad operativa. El GPS y los sistemas GNSS son extraordinariamente útiles, pero no fueron diseñados para ser inmunes a todas las condiciones físicas, ambientales o deliberadas. En este módulo se desarrollará por qué la señal puede degradarse, qué factores afectan el posicionamiento, cómo interpretar el riesgo real y por qué la confianza operacional depende de validar información y no únicamente de recibirla.

2.1 ¿Por qué el GPS es vulnerable?

El GPS y los sistemas GNSS modernos dependen de principios físicos extremadamente precisos: sincronización temporal, propagación de señales de radiofrecuencia, geometría satelital y capacidad del receptor para distinguir señales legítimas muy débiles dentro de un entorno electromagnético complejo. Precisamente por la naturaleza de su funcionamiento, existen múltiples factores que pueden afectar disponibilidad, precisión, estabilidad, continuidad y autenticidad de la señal. La vulnerabilidad GNSS no es una anomalía ni un defecto accidental; es una consecuencia natural de cómo opera el sistema. Entenderlo permite dejar de ver las pérdidas de señal como “misterios” y comenzar a interpretarlas desde una perspectiva técnica, operacional y de riesgo.

Debilidad natural de la señal

Uno de los aspectos menos comprendidos del GPS es la enorme fragilidad física de la señal satelital. Aunque muchas personas suponen que las señales GNSS son fuertes por provenir de satélites avanzados y sistemas globales sofisticados, la realidad es la contraria: la señal debe recorrer aproximadamente entre 19,000 y 23,000 kilómetros desde la órbita media terrestre hasta el receptor, atravesando atmósfera, capas ionosféricas, humedad, ruido electromagnético y otras condiciones físicas que atenúan su energía. Cuando finalmente llega al dispositivo, su potencia de recepción es mínima. Esa debilidad explica por qué pequeñas interferencias, instalaciones deficientes o entornos complejos pueden degradar significativamente el posicionamiento. Desde una perspectiva operacional, esta condición también explica por qué dispositivos relativamente pequeños pueden bloquear, saturar o perturbar la recepción de una señal legítima cuya potencia en superficie ya es extremadamente tenue.

Dependencia de radiofrecuencia

El GNSS depende completamente del espectro electromagnético, ya que la comunicación entre satélite y receptor ocurre mediante radiofrecuencia en bandas específicas para navegación, sincronización y posicionamiento. Esta dependencia convierte al sistema en especialmente sensible a cualquier alteración del entorno RF. El receptor no opera en aislamiento: comparte un espacio electromagnético saturado por antenas, redes celulares, Wi-Fi, radares, enlaces industriales, electrónica de potencia y múltiples fuentes de ruido. En ese contexto, las señales pueden competir, mezclarse, reflejarse o degradarse. Además, esta dependencia RF vuelve al GPS un objetivo relativamente accesible para interferencia intencional. Un jammer no necesita atacar la constelación ni comprometer el satélite; le basta con generar suficiente ruido local para impedir que el receptor distinga correctamente la señal legítima. Esa asimetría operacional es una de las razones centrales de la vulnerabilidad GNSS: un sistema global de enorme complejidad puede verse afectado por un emisor local de bajo costo.

Sensibilidad ambiental

El GPS no opera en un vacío perfecto, sino dentro de un entorno físico complejo y dinámico. Obstáculos como concreto, acero, montañas, túneles, patios cerrados, puentes, infraestructura industrial y zonas urbanas densas limitan la línea de vista con los satélites y reducen la estabilidad de recepción. A ello se suman fenómenos de reflexión, rebote y distorsión, así como variaciones atmosféricas e ionosféricas que alteran la propagación de la señal. En muchos casos, ningún factor aislado provoca por sí solo una falla evidente; es la suma de pequeñas degradaciones la que termina afectando estabilidad, precisión o continuidad. Esta sensibilidad acumulativa es operacionalmente relevante porque explica por qué un evento aparentemente simple puede responder a una combinación de entorno físico, geometría satelital, instalación deficiente, condiciones meteorológicas y saturación electromagnética.

Sensibilidad acumulativa

2.2 Factores que afectan el posicionamiento

El posicionamiento GNSS nunca ocurre de manera permanente en condiciones ideales. La calidad de una posición depende de múltiples variables físicas, ambientales, urbanas, electrónicas y operativas. Comprender estos factores es fundamental para evitar falsas interpretaciones, diagnósticos incorrectos y escalamiento innecesario de incidentes. No toda pérdida GPS es un ataque, pero tampoco toda degradación es accidental. La clave está en comprender contexto, comportamiento, recurrencia espacial y coherencia multisensor para diferenciar entre una condición normal del entorno y una anomalía con posible relevancia operativa.

Clima

Las condiciones climáticas y atmosféricas pueden influir en la propagación de las señales GNSS. La lluvia intensa, las tormentas eléctricas y ciertas perturbaciones ionosféricas asociadas a actividad solar pueden introducir atenuación parcial, ruido adicional, variaciones temporales de precisión o degradación de sincronización. En la mayoría de los casos, estos efectos no bastan por sí solos para inutilizar el sistema, pero sí pueden amplificar otros factores de error ya presentes. Desde el punto de vista operacional, esto significa que la meteorología no debe analizarse como una explicación

única y automática, sino como una variable que modifica el comportamiento del sistema y que puede volver más sensible a la operación frente a errores acumulativos.

Infraestructura

La infraestructura urbana y logística es uno de los factores más importantes de degradación GNSS. Edificios altos, puentes, terminales, patios cerrados, bodegas, estacionamientos subterráneos y estructuras metálicas densas pueden bloquear parcialmente la señal, reducir la visibilidad satelital y generar reflexiones que alteran el cálculo de posición. El sistema funciona mejor con visibilidad relativamente abierta hacia el cielo; por ello, cuanto más cerrado o complejo es el entorno físico, mayor es la probabilidad de pérdida de continuidad, error de posición o inestabilidad temporal. Este punto es especialmente relevante en operaciones de transporte, ya que muchas anomalías observadas en patios, centros de distribución o corredores industriales pueden responder a condiciones estructurales previsibles y no necesariamente a una intervención hostil.

Urbanización

Las ciudades modernas son entornos especialmente complejos para GNSS. Los llamados “cañones urbanos”, formados por edificios altos y calles estrechas, reducen la cantidad de satélites visibles y aumentan la probabilidad de reflexión y recepción no directa. Esto puede producir posiciones desplazadas, saltos aparentes, trayectorias inconsistentes y falsa movilidad. A ello se suma la saturación electromagnética propia de zonas densamente conectadas, donde conviven telecomunicaciones, redes inalámbricas, infraestructura electrónica y una alta concentración de fuentes RF. En consecuencia, la urbanización no sólo dificulta la recepción; también complica la interpretación operativa de las anomalías, ya que un mismo patrón puede parecer sospechoso sin que necesariamente exista una acción deliberada.

Multipath

El multipath es uno de los fenómenos más importantes y menos comprendidos del posicionamiento satelital. Ocurre cuando la señal no llega directamente al receptor, sino después de reflejarse en superficies como edificios, vidrio, metal o infraestructura industrial. El receptor puede interpretar esa señal reflejada como si fuera legítima y directa, lo que introduce errores de tiempo y distancia que terminan desplazando la posición calculada. Operacionalmente, el multipath puede generar trayectorias erráticas, desvíos aparentes, falsa movilidad o pérdida momentánea de precisión, y por ello suele confundirse con manipulación, spoofing o comportamiento anómalo. Comprender este fenómeno es clave para reducir falsos positivos y para distinguir entre errores del entorno urbano y señales potencialmente hostiles.

Túneles y zonas de sombra

Las señales GNSS requieren una línea de vista relativamente abierta con los satélites. Cuando el receptor entra en túneles, pasos subterráneos, zonas montañosas, patios cerrados o estructuras densas, la señal puede desaparecer parcial o totalmente. Dependiendo del dispositivo, esto puede traducirse en congelamiento de la última posición, estimaciones de movimiento, degradación de precisión o pérdida completa de posicionamiento. Desde la perspectiva del monitoreo, estas zonas son críticas porque muchas pérdidas normales de señal pueden parecer eventos sospechosos si no

existe contexto geoespacial adecuado. Por ello, una operación madura debe incorporar mapas de sombra, conocimiento de infraestructura y patrones históricos para interpretar correctamente este tipo de eventos.

Cuando el receptor entra a:

- **túneles,**
- **pasos subterráneos,**
- **zonas montañosas,**
- **patios cerrados,**
- **o estructuras densas,**
  la señal puede desaparecer parcial o totalmente.
-

2.3 Vulnerabilidad vs inutilidad

Uno de los errores más peligrosos en operaciones logísticas es asumir que, si el GPS puede fallar o degradarse, entonces no sirve. Esa conclusión es incorrecta. Toda tecnología posee vulnerabilidades y el objetivo no es eliminar completamente el riesgo —lo cual es imposible— sino comprenderlo, gestionarlo, mitigarlo y construir resiliencia alrededor de él. A pesar de sus límites, el GNSS sigue siendo una de las herramientas más importantes de la logística moderna, un componente crítico de seguridad operacional y una base esencial de trazabilidad. El problema no es utilizar GPS; el problema es depender exclusivamente de él sin validación adicional. Por eso la diferencia entre una operación frágil y una operación resiliente no está en la ausencia de vulnerabilidad, sino en la capacidad de correlacionar múltiples fuentes, comprender la incertidumbre, interpretar el comportamiento y mantener continuidad aun bajo degradación parcial.

2.4 Integridad de señal

La pregunta más importante en el monitoreo moderno ya no es simplemente si existe señal, sino si esa señal puede considerarse confiable. La integridad de señal se relaciona con la capacidad de asumir que la información recibida representa razonablemente la realidad, mantiene coherencia física y posee suficiente calidad para sustentar decisiones. El problema central es la falsa confianza: un sistema puede mostrar una posición estable y aparentemente normal mientras la información es incorrecta, degradada o manipulada. Por ello, la simple existencia de datos no garantiza autenticidad. La integridad debe evaluarse mediante coherencia temporal, coherencia espacial, correlación multisensor y contexto operacional. Una trayectoria que no coincide con telemetría, ignición, CAN Bus, odómetro, horario, carga o zona geográfica debe interpretarse como una señal de duda, no como una verdad automática. En el nuevo paradigma de integridad, las operaciones modernas deben aprender a comprender, validar, correlacionar y cuestionar críticamente la información, porque en entornos vulnerables incluso los datos aparentemente normales pueden formar parte del problema.

Módulo 3. Taxonomía de amenazas GNSS y RF

Uno de los errores más comunes en operaciones de monitoreo consiste en utilizar el término “pérdida GPS” como si todas las alteraciones de señal fueran equivalentes. En la práctica, no lo son. Existen múltiples fenómenos capaces de afectar el posicionamiento, la navegación, la

sincronización temporal, la transmisión de datos y la visibilidad operacional, y cada uno posee mecanismos, indicadores, implicaciones y respuestas distintas. Algunos eventos son accidentales o ambientales; otros son deliberados; algunos derivan de deficiencias técnicas internas; y otros forman parte de estrategias criminales más sofisticadas. Por ello, antes de construir protocolos de respuesta, resulta indispensable clasificar correctamente las amenazas y desarrollar un lenguaje común que permita interpretar la naturaleza real de cada anomalía. Una taxonomía bien construida reduce falsos positivos, evita diagnósticos simplistas y mejora la calidad de la toma de decisiones, porque no es lo mismo enfrentar una degradación urbana, un fallo técnico, un jammer, una manipulación interna o un ataque híbrido coordinado. El objetivo de este módulo es precisamente construir esa comprensión estructurada sobre las amenazas que afectan la integridad operacional del monitoreo moderno.

3.1 Amenazas no intencionales

Las amenazas no intencionales son alteraciones que afectan el posicionamiento o la comunicación sin que exista necesariamente una acción deliberada de ataque. Son especialmente importantes porque muchos eventos legítimos pueden confundirse con incidentes criminales si se interpretan fuera de contexto. Comprender esta categoría permite reducir falsos positivos, evitar escalamiento innecesario y mejorar la precisión operativa del monitoreo. En la práctica, una parte significativa de las degradaciones GNSS cotidianas pertenece a este grupo y se relaciona con saturación del entorno RF, complejidad urbana, infraestructura deficiente, instalaciones incorrectas o mantenimiento insuficiente. El punto central no es minimizar estos eventos, sino comprender que su impacto puede ser real aun cuando su origen no sea hostil. Desde una perspectiva táctica, una operación madura debe ser capaz de diferenciar una condición ambiental o técnica de una interferencia deliberada, ya que la calidad de esa distinción condiciona toda la respuesta posterior.

Saturación RF

El espectro electromagnético moderno se encuentra altamente saturado, especialmente en entornos urbanos e industriales donde conviven antenas, telecomunicaciones, enlaces inalámbricos, redes celulares, dispositivos electrónicos, sistemas industriales y múltiples emisiones electromagnéticas simultáneas. En ese contexto, el receptor GNSS debe distinguir señales satelitales extremadamente débiles dentro de un entorno lleno de ruido, competencia espectral y perturbaciones locales. Cuando el ruido electromagnético aumenta, disminuye la claridad de recepción, se dificulta el seguimiento de la señal y pueden aparecer degradaciones temporales de precisión, retrasos o comportamiento errático. Operacionalmente, la saturación RF suele ser intermitente, afecta zonas específicas, no sigue patrones criminales claros y frecuentemente coexiste con otros factores urbanos. Precisamente por eso resulta peligrosa para el análisis: puede parecer una interferencia deliberada sin serlo, o puede enmascarar un evento más relevante si no existe una lectura contextual adecuada.

Interferencia urbana

Las ciudades modernas son entornos especialmente complejos para GNSS porque alteran de manera constante la propagación, visibilidad, reflexión y estabilidad de la señal. Edificios altos, infraestructura metálica, corredores estrechos tipo cañón urbano, puentes, patios logísticos, puertos y complejos industriales reducen el número de satélites visibles, generan rebotes y aumentan la

probabilidad de errores de posición o trayectorias inconsistentes. El problema operacional radica en que esta interferencia urbana puede producir síntomas similares a degradación sospechosa, jamming parcial o incluso spoofing aparente, aun cuando su origen esté en el entorno físico y no en una acción hostil. Por ello, el contexto geográfico es fundamental: sin conocimiento del terreno, de la infraestructura y de los patrones históricos de comportamiento, una organización corre el riesgo de sobrerreaccionar ante anomalías normales o, por el contrario, de subestimar señales relevantes.

Errores de infraestructura

No todas las anomalías provienen del entorno satelital o del espacio radioeléctrico externo; con frecuencia, la propia infraestructura de la organización genera problemas que luego son interpretados erróneamente como amenazas externas. Mala instalación de antenas, cercanía excesiva con superficies metálicas, obstrucciones físicas, deficiencias eléctricas, variaciones de voltaje, hardware degradado, conectores deteriorados, cableado defectuoso o firmware inestable pueden producir falsas pérdidas, posiciones erráticas, eventos inconsistentes y degradación sostenida del desempeño. Esta categoría es estratégicamente relevante porque muchas organizaciones interpretan automáticamente cualquier anomalía como un posible ataque, cuando en realidad la falta de mantenimiento tecnológico también puede generar incertidumbre, saturación operativa y falsas investigaciones. Una taxonomía madura exige reconocer que la vulnerabilidad no sólo viene de fuera: también puede construirse desde adentro por deficiencia técnica, diseño deficiente o mantenimiento insuficiente.

3.2 Amenazas intencionales

Las amenazas intencionales buscan alterar deliberadamente la navegación, el monitoreo, la trazabilidad, la sincronización o la visibilidad operacional para generar ventaja táctica u operativa. Aquí ya no hablamos de degradaciones accidentales, sino de acciones orientadas a negar, manipular o explotar la confianza tecnológica de la organización. Esta categoría incluye fenómenos como jamming, spoofing, meaconing, repetidores ilegales y ataques híbridos. Su peligrosidad no reside únicamente en el daño técnico que provocan, sino en la forma en que degradan la capacidad de decidir con fundamento. A diferencia de las anomalías ambientales, estas amenazas pueden estar diseñadas para ocultar movimientos, retrasar reacciones, romper la trazabilidad o inducir interpretaciones falsas de la realidad operativa.

- navegación,
- monitoreo,
- trazabilidad,
- sincronización,
- o visibilidad operacional.
-

Jamming

El jamming consiste en interferir deliberadamente la recepción GNSS mediante generación de ruido electromagnético o elevación artificial del nivel de ruido en las bandas de interés, de modo que el receptor no pueda escuchar, interpretar o procesar correctamente la señal legítima. En términos operativos, su objetivo suele ser provocar ceguera temporal, romper la trazabilidad, generar incertidumbre y reducir la capacidad de reacción. Entre sus características más comunes se

encuentran la pérdida abrupta de señal, la caída simultánea de múltiples satélites, interrupciones localizadas y eventos de duración breve o intermitente. Desde una perspectiva criminológica, el jammer frecuentemente no es el objetivo final, sino una herramienta para ocultar movimientos, facilitar un robo o disminuir la capacidad de seguimiento de la organización durante una ventana crítica.

Spoofing

El spoofing consiste en falsificar señales GNSS para engañar al receptor. A diferencia del jamming, aquí no se niega la información: se manipula la percepción del sistema. El receptor puede creer que está recibiendo señales legítimas, cuando en realidad procesa información falsa capaz de producir posiciones incorrectas, trayectorias irreales, velocidades alteradas o tiempos manipulados. Su riesgo estratégico es particularmente alto porque la organización puede creer que todo funciona con normalidad mientras la realidad operacional ya ha sido distorsionada. Precisamente por ello, el spoofing suele ser más difícil de detectar que el jamming: en lugar de producir ausencia visible de datos, puede sostener una apariencia creíble de estabilidad.

Meaconing

El meaconing es una forma de manipulación en la que señales GNSS legítimas son capturadas, retransmitidas o reutilizadas para inducir errores temporales o espaciales en el receptor. A diferencia del spoofing clásico, donde la señal falsa es generada artificialmente, en el meaconing la señal auténtica es desplazada, repetida o reenviada con modificaciones de tiempo o trayectoria. Esto puede generar desplazamientos aparentes, retrasos temporales y alteraciones difíciles de detectar, especialmente cuando la señal retransmitida conserva rasgos legítimos. Por ello, el meaconing representa una amenaza sutil: aprovecha la credibilidad de la señal auténtica para producir engaño operacional.

Repetidores ilegales

Algunos dispositivos retransmiten señales GNSS hacia interiores o zonas bloqueadas. Aunque ciertos repetidores pueden tener usos técnicos muy controlados, los repetidores ilegales generan distorsiones, ecos, errores de sincronización y degradaciones operativas que pueden parecer spoofing parcial o interferencia anómala. En la práctica, estos dispositivos pueden producir trayectorias inconsistentes, posiciones inestables y comportamientos difíciles de interpretar desde el centro de monitoreo. Su relevancia dentro de la taxonomía radica en que ocupan una zona gris entre el problema técnico y la amenaza operacional: no siempre buscan engañar activamente, pero sí pueden degradar seriamente la confiabilidad del sistema.

Ataques híbridos

Las amenazas modernas rara vez ocurren de forma aislada. Los actores más sofisticados combinan múltiples mecanismos simultáneamente, por ejemplo jamming junto con inhibición celular, spoofing acompañado de manipulación telemática, pérdida GNSS asociada a sabotaje interno o interferencia RF combinada con desvío operacional. Estos ataques híbridos son especialmente peligrosos porque dificultan el diagnóstico, aumentan la incertidumbre, retrasan la respuesta y generan múltiples capas de confusión. Su característica principal es que buscan destruir la

capacidad de correlación de la organización: cuando todas las fuentes parecen inconsistentes al mismo tiempo, se erosiona la confianza operacional y se amplía la ventana de maniobra del adversario. En términos de resiliencia, esta categoría obliga a pensar en arquitectura, procesos y validación multisensor, no sólo en detección de una señal aislada.

3.3 Amenazas internas

No todas las amenazas provienen del exterior. Muchas alteraciones operativas involucran participación interna, negligencia, manipulación deliberada o sabotaje organizacional. Ignorar esta posibilidad genera puntos ciegos críticos, porque el actor interno conoce procesos, tiempos, protocolos, vulnerabilidades tecnológicas y rutinas operativas. Esta categoría no sólo incluye conductas maliciosas, sino también acciones que, sin un ataque RF sofisticado, pueden degradar gravemente la capacidad de monitoreo, trazabilidad y respuesta. Desde una perspectiva estratégica, las amenazas internas son especialmente delicadas porque operan desde la proximidad: conocen cómo funciona el sistema y dónde puede romperse con el menor esfuerzo.

Sabotaje

El sabotaje implica afectar deliberadamente equipos, infraestructura, conectividad o trazabilidad para debilitar la capacidad de monitoreo y control. Puede manifestarse como daño físico a antenas, alteración de instalaciones, manipulación eléctrica, bloqueo intencional o desconexión deliberada de componentes críticos. Sus motivaciones pueden ir desde robo interno y encubrimiento hasta corrupción, venganza laboral o colusión criminal. El sabotaje interno no siempre requiere sofisticación técnica avanzada; en muchos casos, basta con conocer dónde intervenir para producir incertidumbre operacional suficiente. Su relevancia radica en que puede simular una falla externa y desviar la investigación hacia hipótesis equivocadas si no se consideran adecuadamente los factores internos.

- equipos,
- infraestructura,
- conectividad,
- o trazabilidad.

Manipulación deliberada

Algunas alteraciones internas no buscan destruir el sistema, sino modificar la interpretación operacional que la organización hace de sus propios datos. La manipulación deliberada puede incluir cambios manuales de configuración, alteración de eventos, eliminación de registros, modificación de telemetría o uso indebido de herramientas administrativas para alterar la narrativa visible en plataforma. Su efecto no siempre es inmediato o espectacular; precisamente por eso puede ser más difícil de detectar. Se trata de una amenaza orientada a distorsionar la verdad operacional desde dentro del sistema, afectando tanto la toma de decisiones en tiempo real como la reconstrucción posterior de los hechos.

Desconexión operativa

Una amenaza interna frecuente consiste en desactivar parcial o totalmente la capacidad de monitoreo sin necesidad de introducir interferencia externa sofisticada. Esto puede incluir

desconexión física, inhibición energética, retiro de antenas, bloqueo deliberado de transmisión o cualquier otra acción orientada a romper la continuidad informativa. El riesgo estratégico de esta categoría es alto porque aprovecha conocimiento interno sobre procesos, dependencias y tiempos de reacción. Cuando la desconexión operativa ocurre desde dentro, la organización puede tardar más en comprender si enfrenta una falla técnica, una negligencia o un acto deliberado, ampliando así la ventana de vulnerabilidad.

3.4 Amenazas combinadas

En entornos reales, las amenazas rara vez aparecen aisladas. La combinación de múltiples alteraciones genera escenarios mucho más complejos porque mezcla negación de servicio, degradación de señal, pérdida de comunicación, manipulación telemática, sabotaje interno y desvío físico en una misma secuencia operativa. Esta categoría merece atención especial porque las amenazas combinadas están diseñadas para dificultar el diagnóstico, aumentar la incertidumbre y destruir la capacidad de correlación de la organización. Cuando varias capas de información fallan o se contradicen simultáneamente, la empresa no sólo pierde visibilidad: pierde confianza en su propio criterio de interpretación.

Bloqueo GNSS + inhibición celular

Este es uno de los escenarios más comunes y peligrosos en eventos criminales. Cuando el GNSS deja de funcionar y, simultáneamente, la transmisión celular también desaparece, la organización pierde ubicación, comunicación y capacidad de visibilidad casi al mismo tiempo. El resultado es una ruptura de seguimiento que genera incertidumbre extrema y abre ventanas críticas para la acción adversaria. La gravedad de este escenario radica en que niega tanto la capa de posicionamiento como la capa de transmisión, dejando al centro de monitoreo con muy pocas fuentes inmediatas para validar lo que ocurre.

Manipulación multisistema

Las operaciones modernas dependen de múltiples tecnologías interconectadas, por lo que las amenazas también evolucionan hacia múltiples capas de manipulación. Alteración de GPS junto con falsificación de CAN Bus, interferencia GNSS acompañada de manipulación telemática, desvío físico combinado con spoofing digital o sabotaje interno sumado a pérdida RF son ejemplos de cómo puede destruirse la capacidad de correlación. La característica central de la manipulación multisistema es precisamente esa: cuando todas las fuentes parecen inconsistentes entre sí, la organización pierde confianza operacional y se vuelve más difícil distinguir la realidad del engaño. En términos tácticos, esta categoría exige modelos de validación más robustos y criterios más finos de interpretación multisensor.

3.5 Impacto operacional de las amenazas RF

Las amenazas GNSS y RF no afectan únicamente tecnología; afectan decisiones, continuidad, seguridad y capacidad operativa. Su impacto más grave aparece cuando la organización pierde conciencia situacional y deja de comprender con suficiente certeza qué está ocurriendo. A partir de ese momento, el problema deja de ser técnico para convertirse en un problema de gobernanza

operativa. Cuando la información deja de ser confiable, el monitoreo se satura, la reacción se retrasa, la trazabilidad se fragmenta y la toma de decisiones se degrada. Por ello, el verdadero impacto de las amenazas RF no se mide sólo por la pérdida de señal, sino por la pérdida de capacidad para actuar con fundamento sobre la realidad operativa.

Pérdida de visibilidad

La visibilidad operacional depende de información confiable, continuidad y coherencia entre fuentes. Cuando las señales se degradan o son manipuladas, la organización pierde capacidad de observar correctamente lo que ocurre y entra en un estado de incertidumbre que afecta la respuesta táctica. Esto puede traducirse en retrasos, escalamiento innecesario, ceguera temporal, saturación del centro de monitoreo y aumento general del riesgo. La pérdida de visibilidad no siempre significa ausencia total de datos; a veces significa algo más peligroso: contar con datos que ya no pueden interpretarse con confianza.

Ruptura de trazabilidad

La trazabilidad permite reconstruir movimientos, tiempos, decisiones y eventos. Cuando la integridad GNSS se rompe, aparecen vacíos operativos que dificultan la auditoría, debilitan la evidencia y complican la reconstrucción posterior de los hechos. Esta ruptura afecta tanto la operación en tiempo real como la investigación posterior, porque sin continuidad informativa se vuelve más difícil distinguir qué ocurrió, cuándo ocurrió y bajo qué condiciones. En términos organizacionales, la ruptura de trazabilidad no sólo debilita el control; también erosiona la capacidad de aprendizaje posterior al incidente.

Afectación de continuidad

Las operaciones modernas dependen profundamente del monitoreo, la sincronización, la coordinación y la visibilidad. Cuando la información deja de ser confiable, la continuidad operacional se degrada: aumenta la carga de trabajo, se saturan los equipos de monitoreo, se elevan los costos, crece el riesgo reputacional y se debilita la confianza en el sistema. El problema más grave no es únicamente perder señal, sino perder capacidad de comprender con certeza qué está ocurriendo. Y cuando una organización pierde confianza en su información, también pierde capacidad de decisión, de reacción y de anticipación. En operaciones logísticas modernas, esa incertidumbre es en sí misma una forma de vulnerabilidad.

PARTE II — DETECTAR

Módulo 4. Interferencia deliberada: Jamming

El jamming representa una de las formas más directas y operativamente peligrosas de interferencia deliberada contra sistemas GNSS. A diferencia de una degradación ambiental o de una falla interna del equipo, aquí existe una intención clara de negar o degradar la recepción de la señal para romper la continuidad del monitoreo y reducir la capacidad de reacción de la organización. En el contexto logístico, el jamming no debe analizarse únicamente como un problema técnico de radiofrecuencia, sino como una táctica de ocultamiento operacional que puede abrir ventanas de oportunidad para desvíos, inmovilizaciones, robos o manipulación de la trazabilidad. Este módulo tiene como propósito explicar qué es un jammer, cómo funciona, qué indicadores técnicos y operativos suelen acompañarlo, y de qué manera una organización puede detectar y responder con mayor criterio ante este tipo de evento. Las recomendaciones de organismos oficiales sobre resiliencia PNT insisten en

que la dependencia de una sola fuente de posicionamiento es una debilidad estructural y que la detección efectiva exige corroboración, validación contextual y continuidad operativa basada en redundancia.

4.1 ¿Qué es un jammer?

Un jammer es un emisor de radiofrecuencia diseñado para interferir la recepción legítima de señales GNSS, elevando artificialmente el nivel de ruido o introduciendo perturbaciones suficientes para que el receptor deje de procesar con normalidad la señal satelital. Su función no consiste en afectar físicamente los satélites ni en alterar la constelación en el espacio, sino en degradar localmente la capacidad del receptor para escuchar, seguir y resolver correctamente la información que recibe. Debido a que las señales GNSS llegan a la superficie terrestre con una potencia extremadamente baja, incluso una fuente de interferencia relativamente pequeña puede generar efectos significativos sobre la navegación, la sincronización y la posición disponible para la operación. Desde la perspectiva logística, el jammer es relevante no sólo por el daño técnico que ocasiona, sino porque crea una zona temporal de opacidad operativa en la que la organización pierde confianza en su visibilidad.

4.2 ¿Cómo funciona el jamming?

El jamming funciona por saturación del entorno radioeléctrico. El receptor GNSS necesita distinguir señales muy débiles en bandas específicas de navegación y sincronización; cuando aparece una fuente de ruido suficientemente intensa o cercana, la relación señal-ruido se degrada hasta el punto en que el equipo pierde estabilidad de seguimiento. En términos prácticos, esto puede traducirse en pérdida de portadora, caída de códigos de seguimiento, disminución del número de satélites utilizables, degradación rápida de precisión o ausencia total de solución válida. La lógica física detrás del fenómeno es clave para comprender su peligrosidad: no se requiere una gran infraestructura para afectar la recepción, porque el sistema legítimo ya opera cerca del límite de sensibilidad del receptor. Por ello, el jamming puede ser breve, localizado y aun así producir consecuencias operativas desproporcionadas, especialmente si coincide con zonas de riesgo, momentos críticos o eventos de seguridad en curso.

4.3 Tipologías de jammer

Desde una perspectiva operativa, conviene clasificar los jammers no sólo por su tecnología, sino también por su forma de despliegue, cobertura y persistencia. Esta clasificación resulta útil porque no todos los escenarios de interferencia representan el mismo nivel de riesgo ni exigen la misma respuesta. Existen dispositivos portátiles asociados con ventanas cortas de interferencia y proximidad inmediata; equipos vehiculares que acompañan movimientos y pueden sostener negación de señal a lo largo de un corredor; emisores de mayor potencia capaces de ampliar el radio de afectación; y configuraciones multibanda que comprometen simultáneamente varias frecuencias de uso GNSS. Aunque la taxonomía específica puede variar según el entorno, la lógica común es que el impacto del jamming depende de la potencia radiada, la distancia al receptor, la geometría de exposición y la banda o bandas afectadas. Cuanto mayor sea la capacidad de cubrir espacio, tiempo y múltiples frecuencias, mayor será la dificultad para recuperar continuidad y validar rápidamente la realidad operativa.

4.4 Impacto operativo del jamming

El impacto operativo del jamming no debe medirse solamente por la duración de la pérdida de señal, sino por la degradación de conciencia situacional que produce y por las acciones que esa ceguera temporal permite ejecutar a terceros. Cuando una unidad entra en una zona de interferencia, el centro de monitoreo puede perder posición, estabilidad de ruta, precisión o continuidad de eventos, lo que rompe la capacidad de interpretar lo que realmente está ocurriendo. En logística, esta pérdida de visibilidad puede traducirse en retrasos de reacción, errores de escalamiento, debilitamiento de la trazabilidad y apertura de ventanas de oportunidad criminal para desvíos, inmovilizaciones, transbordos o desaparición digital temporal. En otras palabras, el jamming no sólo afecta una señal: afecta la capacidad de gobernar la operación en tiempo real.

4.5 Indicadores técnicos de jamming

Los indicadores técnicos de jamming suelen caracterizarse por una degradación abrupta y poco coherente con el comportamiento normal del equipo o del entorno. Entre los signos más relevantes se encuentran la pérdida súbita de recepción GNSS, la reducción inesperada del número de satélites utilizables, la caída de precisión, la transición rápida de estados válidos a no fix, el congelamiento de posición o la aparición de comportamiento errático inmediatamente antes de la pérdida total de navegación. También resulta importante observar la coherencia espacial y temporal del evento: cuando la degradación aparece de forma localizada, repetitiva y concentrada en un corredor o ventana horaria concreta, la hipótesis de interferencia deliberada gana fuerza frente a una simple falla progresiva del equipo. Desde el punto de vista del análisis, ningún indicador aislado es concluyente por sí mismo; lo valioso es la convergencia entre síntomas técnicos, entorno geográfico y contexto operativo.

Otro indicador clave es el patrón RF: el problema suele aparecer de forma súbita, localizada y con coherencia espacial limitada a un corredor, una zona o una ventana de tiempo específica. Eso ayuda a diferenciarlo de una simple falla progresiva del equipo. La guía de GPS.gov también recuerda que la interferencia puede venir de emisiones en bandas cercanas, jamming intencional o no intencional, y de space weather; por eso, la detección técnica debe distinguir entre causas distintas antes de escalar.

4.6 Indicadores operativos

Los indicadores operativos del jamming surgen cuando la anomalía técnica se conecta con patrones de comportamiento en ruta, temporalidad y contexto de riesgo. Una pérdida GNSS aislada puede ser ruido; una secuencia recurrente en el mismo corredor, a horarios semejantes o bajo condiciones operativas similares, ya constituye una señal de riesgo que merece análisis estructurado. También son relevantes las inconsistencias entre la pérdida de posicionamiento y el resto del comportamiento de la unidad: desaparición simultánea de GPS y comunicación, detención abrupta sin explicación operativa, reaparición en un punto incoherente, ruptura de trazabilidad en zonas críticas o contradicciones entre ruta, velocidad y telemetría. La clave está en comprender que el jamming rara vez se presenta como un dato abstracto; se manifiesta como una alteración técnica con consecuencias prácticas sobre la lógica de la operación. Por ello, el monitoreo maduro convierte

recurrencias y anomalías repetidas en inteligencia de corredores, horarios críticos y tipologías de exposición.

4.7 Detección avanzada de interferencia

La detección avanzada de interferencia exige abandonar la dependencia exclusiva del punto mostrado en el mapa y adoptar una lógica de correlación multisensor y validación contextual. Ante una posible disrupción GNSS, las recomendaciones de resiliencia PNT señalan la importancia de utilizar fuentes alternas o complementarias, como sensores a bordo, telemetría, otras constelaciones, datos de red y referencias temporales adicionales, para determinar si la información recibida mantiene coherencia con la realidad física de la operación. En términos prácticos, detectar jamming de manera madura implica contrastar el comportamiento GNSS con ignición, movimiento real, eventos del vehículo, patrón de ruta, contexto geográfico e historial del corredor. También implica discriminar entre un entorno difícil —por ejemplo, zonas urbanas densas o infraestructura que complica recepción— y una interferencia deliberada con patrones súbitos, localizados y repetitivos. La detección avanzada no consiste sólo en reconocer una caída de señal; consiste en comprender cuándo esa caída forma parte de un entorno operacional hostil y cuándo debe tratarse como un incidente de seguridad con posible relevancia táctica.

4.8 Respuesta operativa ante jamming

La respuesta operativa ante jamming debe comenzar con confirmación razonada del evento y no con suposición automática. Antes de escalar, es necesario valorar si la pérdida de señal puede explicarse por entorno, falla técnica, desconexión interna o interferencia deliberada. Una vez superado ese primer filtro, la organización debe activar un esquema de escalamiento coherente entre monitoreo, seguridad, operaciones y liderazgo, de modo que todos interpreten el incidente bajo los mismos criterios. Las guías de resiliencia PNT enfatizan que, frente a una disrupción, deben utilizarse fuentes alternas o complementarias y mantenerse la continuidad conforme a planes previamente definidos, no mediante improvisación. Esto implica sostener operación con reglas de contingencia, reforzar validación de telemetría y contexto, documentar cronología del evento y preservar todos los registros útiles para investigación posterior. La respuesta madura no se limita a intentar “recuperar señal”; busca confirmar, contener, mantener conciencia situacional, proteger evidencia y aprender del incidente para reducir exposición futura.

Cierre del módulo

Comprender el jamming implica reconocer que no toda pérdida de GPS es una simple falla técnica ni toda degradación debe interpretarse de manera aislada. El verdadero reto consiste en identificar cuándo la organización está enfrentando un entorno RF hostil que ya compromete su capacidad de navegar, monitorear y decidir con fundamento. Las referencias oficiales coinciden en tres ideas centrales: la señal GNSS es débil, el espectro que la soporta es vulnerable a interferencias y la resiliencia depende de validación, redundancia y continuidad previamente planificada. Desde esa perspectiva, el valor de este módulo no reside sólo en definir qué es un jammer, sino en desarrollar criterio para reconocer cómo una interferencia deliberada se traduce en riesgo operacional, en pérdida de visibilidad y en necesidad de respuesta estructurada.

Módulo 5. Manipulación de navegación: Spoofing

El spoofing representa una de las amenazas más sofisticadas dentro del ecosistema GNSS porque no busca simplemente negar información, sino manipularla de forma que parezca legítima. Mientras el jamming suele generar ausencia de señal y, por lo tanto, despierta sospecha con relativa rapidez, el spoofing produce un escenario más peligroso: la organización continúa viendo datos, trayectorias y posiciones, pero esos datos pueden no corresponder a la realidad física. Esta capacidad de crear una apariencia de normalidad convierte al spoofing en una amenaza especialmente crítica para operaciones logísticas, donde la confianza en la ubicación, en la secuencia temporal y en la trazabilidad constituye la base de múltiples decisiones de seguridad, auditoría y continuidad.
En términos estratégicos, el spoofing obliga a replantear una idea fundamental: no basta con tener información disponible; es indispensable determinar si esa información es auténtica, coherente y confiable. Cuando una empresa toma decisiones sobre la base de posiciones falsas, el problema ya no es técnico en sentido estricto, sino operacional, investigativo y de gobernanza. Se debilita la capacidad de reaccionar a tiempo, se compromete la validez de los registros y se abre la posibilidad de que auditorías, rutas y evidencias se construyan sobre una narrativa digital incorrecta. Por ello, este módulo desarrolla el spoofing no sólo como una técnica de engaño satelital, sino como una amenaza directa a la integridad de la toma de decisiones y a la resiliencia operacional. **[GPS and GNSS Interference Resource Guide]()** y **[GNSS Spoofing]()** destacan precisamente que el desafío principal de esta amenaza es que puede mantener una apariencia creíble de funcionamiento mientras degrada la confianza en la posición, navegación y tiempo.

5.1 ¿Qué es el spoofing?

El spoofing GNSS es una técnica de engaño en la que un receptor acepta señales falsas o manipuladas como si fueran legítimas, generando una solución incorrecta de posición, velocidad o tiempo sin que necesariamente aparezca una alarma evidente. A diferencia del jamming, cuyo efecto principal es negar o degradar la recepción, el spoofing pretende sustituir la realidad por una narrativa navegacional falsa. El receptor continúa calculando, la plataforma sigue mostrando datos y el sistema aparenta normalidad, pero la información resultante puede no corresponder al movimiento real de la unidad. Esa diferencia entre bloqueo y engaño es esencial: el jamming produce ceguera; el spoofing produce confianza equivocada. **[GNSS Spoofing]()** subraya justamente que este tipo de manipulación puede hacer que los sistemas de rastreo muestren una ubicación y una trayectoria falsas sin que el operador lo advierta de inmediato, mientras que la **[GPS and GNSS Interference Resource Guide]()** destaca que los efectos del spoofing pueden persistir y seguir afectando el comportamiento del receptor incluso después del evento inicial.
Desde una perspectiva operativa, el spoofing busca modificar variables críticas como ubicación, dirección, tiempo, velocidad o secuencia de desplazamiento para inducir rutas aparentes, movimientos inexistentes, tiempos alterados o permanencia ficticia dentro de corredores autorizados. El riesgo más importante no radica únicamente en que el dato sea incorrecto, sino en que ese dato conserve apariencia de legitimidad. Cuando una organización pierde GPS, normalmente sospecha y activa verificación; cuando recibe información falsa pero aparentemente estable, puede seguir operando bajo una percepción equivocada de la realidad. Precisamente ahí se encuentra la peligrosidad superior del spoofing: no interrumpe sólo la señal, interrumpe el criterio mediante el cual la empresa confía en su propia información.

5.2 ¿Cómo funciona el spoofing?

El spoofing funciona mediante la transmisión de señales falsas diseñadas para imitar las características de una señal GNSS auténtica. El atacante intenta que el receptor las perciba como válidas y les otorgue mayor confianza que a la señal legítima recibida desde los satélites. Para lograrlo, puede copiar parámetros creíbles de sincronización, estructura temporal y comportamiento espectral, de manera que el receptor sustituya gradualmente la referencia real por una referencia manipulada. A partir de ese momento, el dispositivo continúa resolviendo navegación, pero lo hace sobre una base falsa. El resultado puede ser una posición desplazada, una trayectoria inventada, una permanencia ficticia en un punto o una alteración del tiempo de referencia. **[GNSS Spoofing]()** explica que este tipo de manipulación puede dirigir sistemas de rastreo hacia ubicaciones erróneas y mostrar caminos falsos, mientras que la **[GPS and GNSS Interference Resource Guide]()** destaca que los efectos del spoofing no siempre terminan de inmediato y pueden dejar al receptor en un estado alterado aun después del evento.

En la práctica, el spoofing puede manifestarse de forma abrupta o progresiva. En su versión más evidente, la posición cambia de manera repentina hacia un punto imposible o incoherente; en formas más sofisticadas, el desplazamiento ocurre lentamente para reducir probabilidad de detección inmediata. También puede concentrarse en la variable temporal y alterar secuencias, marcas de tiempo o velocidad aparente sin generar un salto espacial extremo. Esta variedad operativa vuelve el fenómeno especialmente complejo, porque el receptor no “sabe” automáticamente que está siendo engañado: si las señales falsas parecen suficientemente plausibles, puede aceptarlas como si fueran auténticas. Por ello, la detección del spoofing exige criterios más finos que la simple observación de pérdida de señal.

La plataforma puede mostrar:

Esto suele ser más detectable.

5.3 Impacto del spoofing en logística

El impacto del spoofing en logística es profundo porque altera la base informativa sobre la cual se coordinan rutas, tiempos, auditorías, validaciones y respuestas de seguridad. Cuando una plataforma muestra una ruta que no corresponde al desplazamiento físico real, la organización pierde conciencia situacional sin necesariamente advertirlo. Esto puede traducirse en falsa permanencia dentro de un corredor autorizado, movimiento aparente cuando la unidad está detenida en otro punto, cumplimiento ficticio de hitos de entrega o reconstrucción equivocada de la secuencia operativa. El daño, por tanto, no se limita al mapa: afecta la manera en que la empresa interpreta la realidad y decide sobre ella.

El spoofing también compromete gravemente auditorías, cumplimiento y valor probatorio de los registros. Muchos procesos de validación se apoyan en trayectorias GNSS para demostrar que una unidad estuvo en determinada ubicación, recorrió cierto trayecto o cumplió una ventana de servicio. Si esos datos fueron manipulados, la evidencia resultante puede sostener una narrativa falsa con apariencia documental legítima. Esto afecta investigaciones internas, análisis posteriores al incidente y, en contextos más sensibles, la posibilidad de sustentar decisiones operativas o legales sobre bases confiables. En consecuencia, el spoofing debe entenderse como una amenaza directa contra la integridad de la trazabilidad y no sólo como una anomalía de navegación.

5.4 Indicadores técnicos de spoofing

El spoofing rara vez se detecta mediante un solo síntoma. Su identificación técnica depende de observar acumulación de inconsistencias que resultan incompatibles con la física del movimiento, con la infraestructura o con la secuencia temporal esperada. Entre los indicadores más relevantes se encuentran los saltos imposibles de posición, desplazamientos instantáneos de gran distancia, trayectorias geométricamente artificiales, movimientos sobre zonas inaccesibles, velocidades incompatibles con la realidad operacional y cambios espaciales sin transición lógica. También deben observarse las inconsistencias temporales: eventos fuera de secuencia, marcas de tiempo anómalas, intervalos incoherentes entre posiciones o velocidades que no corresponden al tiempo transcurrido. La clave no está en un dato aislado, sino en la convergencia de patrones incompatibles con un comportamiento auténtico.

Desde la perspectiva analítica, el criterio central es la plausibilidad física. Una posición puede parecer técnicamente válida en la plataforma y, sin embargo, ser operativamente imposible. Por ello, el análisis técnico del spoofing debe incorporar validación de continuidad, estabilidad, secuencia y persistencia. La pregunta no es sólo si el sistema sigue entregando datos, sino si esos datos conservan coherencia con la realidad del entorno. **[Recent Advances on Jamming and Spoofing Detection in GNSS]()** destaca precisamente que la detección temprana depende de combinar métodos y no confiar en un único criterio de verificación, mientras que la **[GPS and GNSS Interference Resource Guide]()** subraya que el spoofing puede sostener una solución aparentemente válida incluso cuando el sistema ya ha sido comprometido.

5.5 Validación multisensor

La validación multisensor constituye una de las defensas más relevantes frente al spoofing porque permite contrastar la narrativa GNSS con fuentes independientes de información. La lógica es sencilla: si múltiples sistemas que observan el comportamiento de la unidad desde principios distintos coinciden entre sí, la confianza aumenta; si se contradicen, la hipótesis de manipulación gana fuerza. En este contexto, el INS aporta estimaciones basadas en acelerómetros y giroscopios; el CAN Bus ofrece variables del comportamiento real del vehículo, como velocidad, frenado, revoluciones o ignición; el odómetro ayuda a verificar distancia efectivamente recorrida; y la telefonía celular puede brindar una referencia geográfica aproximada o regional para contrastar posición. Ninguna de estas fuentes es perfecta por sí sola, pero en conjunto forman una red de coherencia capaz de cuestionar una solución GNSS aparentemente válida.

La utilidad táctica de esta validación radica en su capacidad para revelar contradicciones que el GPS aislado no podría evidenciar. Si el sistema reporta movimiento, pero el odómetro no cambia; si la trayectoria indica desplazamiento, pero el CAN Bus refleja inmovilidad; o si la posición visible no coincide razonablemente con la referencia celular o con la dinámica inercial, la organización obtiene señales fuertes de que la información principal puede estar comprometida. En el contexto del spoofing, la correlación multisensor no es un complemento opcional, sino un mecanismo esencial para determinar si la navegación observada conserva autenticidad física.

5.6 Detección avanzada

La detección avanzada del spoofing exige ir más allá de la observación del punto en el mapa y adoptar una lectura integral del comportamiento del sistema. El criterio central es la coherencia física: si la velocidad no es posible, si la trayectoria contradice la infraestructura disponible, si el tiempo no coincide con la distancia recorrida o si el movimiento visible se opone a señales internas del vehículo, la autenticidad GNSS debe cuestionarse. A esto se suma el análisis temporal, que revisa continuidad, secuencia, persistencia y lógica de eventos, y la correlación dinámica, que integra GPS, telemetría, historial, sensores y contexto operacional para evaluar si el conjunto de datos describe una situación verosímil o una narrativa manipulada.
El objetivo de una detección madura no es encontrar una única señal inequívoca, sino identificar patrones incompatibles con la realidad física. **[Recent Advances on Jamming and Spoofing Detection in GNSS]()** enfatiza que la detección eficaz de spoofing suele depender de enfoques combinados y de validación cruzada, mientras que **[GNSS Spoofing]()** muestra que un sistema independiente de referencia puede advertir cuándo la información visualizada por los dispositivos ya no merece confianza. Esta lógica es especialmente relevante en logística, donde una detección tardía no sólo retrasa la respuesta, sino que permite que el engaño continúe operando bajo apariencia de normalidad.

5.7 Respuesta operativa ante spoofing

La respuesta operativa ante spoofing debe partir de un principio distinto al utilizado frente al jamming: aquí no se enfrenta ausencia de información, sino pérdida de confianza en la autenticidad de la información disponible. Cuando existen indicios razonables de manipulación, la organización debe suspender la confianza automática en la solución GNSS y tratarla como una fuente potencialmente comprometida hasta que sea validada por otros medios. Esto no implica ignorar completamente los datos, sino someterlos a verificación reforzada antes de utilizarlos para decisiones críticas. A partir de ese momento, resulta indispensable activar un escalamiento táctico que involucre monitoreo, seguridad, operaciones e inteligencia, de modo que el evento se interprete bajo criterios comunes y no como una simple anomalía aislada.
Las acciones operativas más relevantes incluyen activar validación multisensor, verificar coherencia con telemetría y comportamiento físico, establecer contacto operativo cuando sea viable, revisar correlación de rutas y preservar de inmediato la evidencia digital útil para análisis posterior. Esto abarca registros GNSS, telemetría, secuencias temporales, historial de eventos y cualquier fuente complementaria que permita reconstruir con mayor fidelidad lo ocurrido. En el spoofing, la preservación de evidencia es particularmente importante porque el ataque puede afectar directamente la credibilidad de los registros. Por ello, una respuesta madura no sólo busca contener el incidente, sino también proteger la capacidad de investigación y aprendizaje posterior. **[GPS and GNSS Interference Resource Guide]()** y **[GNSS Spoofing]()** coinciden en que la continuidad operativa frente a manipulación GNSS depende de verificación independiente, reducción de confianza ciega en la señal y preparación previa para operar con referencias alternas. Y en operaciones modernas, la capacidad de cuestionar críticamente los datoses parte fundamental de la resiliencia operacional.

Módulo 6. Doppler, autenticidad y coherencia física

En el monitoreo logístico moderno, uno de los errores más frecuentes consiste en asumir que el valor principal del GNSS se limita a mostrar una coordenada sobre el mapa. En realidad, los sistemas de navegación satelital contienen información física mucho más rica sobre movimiento, velocidad, sincronización, estabilidad y coherencia dinámica. Entre los elementos más importantes para interpretar esa coherencia se encuentra el efecto Doppler, un fenómeno que permite observar cómo se comporta la señal desde una perspectiva física y no únicamente cartográfica.
Aunque el Doppler suele percibirse como un concepto complejo o exclusivamente técnico, en realidad es una herramienta esencial para validar autenticidad, detectar inconsistencias, identificar manipulación y comprender si el comportamiento observado en una plataforma corresponde a un movimiento físicamente posible. Su valor estratégico radica en que ayuda a responder una pregunta crítica: si la señal que estamos recibiendo se comporta como debería comportarse en el mundo real. En operaciones resilientes, esta pregunta es tan importante como la posición misma, porque una coordenada puede falsificarse con mayor facilidad que una coherencia física completa sostenida en el tiempo. **[Doppler Shift | GEOG 862: GPS and GNSS]()** y **[How does a GNSS receiver estimate velocity?]()** explican que las mediciones Doppler son observables fundamentales para estimar velocidad, validar dinámica y mejorar la interpretación del comportamiento del receptor. Uno de los elementos más importantes para comprender esa coherencia es el efecto Doppler.

6.1 ¿Qué es el efecto Doppler?

El efecto Doppler es un fenómeno físico que describe el cambio aparente de frecuencia de una señal cuando existe movimiento relativo entre el emisor y el receptor. En la vida cotidiana, suele ilustrarse con el sonido de una ambulancia: cuando se acerca, el tono parece más agudo; cuando se aleja, parece más grave. La señal en sí no cambia su naturaleza esencial, pero la forma en que es percibida sí se modifica debido al movimiento. En GNSS ocurre el mismo principio, aunque aplicado a señales de radiofrecuencia emitidas por satélites que se desplazan a gran velocidad respecto del receptor terrestre.
En los sistemas GNSS, el receptor analiza las variaciones Doppler para ayudar a estimar velocidad, sostener seguimiento de portadora, mantener sincronización y mejorar precisión dinámica. Esto significa que el Doppler no es un error ni una distorsión indeseada; por el contrario, es una fuente valiosa de información física sobre cómo se mueve realmente la relación satélite-receptor.
[Doppler Shift | GEOG 862: GPS and GNSS]() explica que el Doppler constituye un observable fundamental para determinar la tasa de cambio de distancia entre satélite y receptor, mientras que **[What Is the Doppler Shift and Why Is It Vital in GNSS/GPS Antennas?]()** resume por qué este fenómeno es clave para que un receptor interprete con precisión movimiento y posición.

6.2 Doppler y posicionamiento

El Doppler no es un elemento secundario del posicionamiento GNSS; forma parte de su funcionamiento práctico. Una de sus aplicaciones más importantes es la estimación de velocidad, ya que el cambio de frecuencia asociado al movimiento relativo entre satélite y receptor permite calcular con gran sensibilidad la dinámica del sistema. En muchos escenarios, la velocidad derivada del Doppler es más estable y precisa que la obtenida únicamente por diferencia entre posiciones consecutivas, especialmente cuando se requiere interpretar movimientos rápidos, transiciones

breves o cambios de trayectoria en tiempo real. **[How does a GNSS receiver estimate velocity?]()** explica precisamente que la velocidad basada en Doppler puede alcanzar una precisión mucho mejor que la derivada sólo de posiciones sucesivas.
Además de la velocidad, el Doppler contribuye a la sincronización del receptor y a la estabilidad general de la navegación. Dado que el GNSS depende críticamente del tiempo, pequeñas alteraciones temporales pueden producir grandes errores espaciales. El análisis Doppler ayuda a mantener consistencia dinámica, refinamiento del cálculo y reducción de incertidumbre. Desde la perspectiva logística, esto permite validar desplazamientos, detectar inconsistencias y analizar no sólo dónde está una unidad, sino cómo se está moviendo. Esa dimensión dinámica del posicionamiento es esencial para distinguir entre un comportamiento físicamente razonable y una narrativa de navegación potencialmente alterada.

6.3 Doppler y autenticidad de señal

Uno de los conceptos más relevantes del monitoreo moderno es la autenticidad física de la señal. Esto significa que la información observada no sólo debe parecer razonable en la plataforma, sino comportarse de manera coherente con las leyes reales del movimiento. El análisis Doppler permite verificar si velocidad, dirección, aceleración y desplazamiento mantienen una lógica dinámica compatible con un trayecto auténtico. Un movimiento legítimo suele producir patrones consistentes: aceleraciones progresivas, cambios de velocidad razonables, trayectorias físicamente posibles y continuidad temporal estable.
Desde esta perspectiva, el Doppler se convierte en una herramienta poderosa para cuestionar la autenticidad de una solución GNSS aparentemente válida. Falsificar una posición aislada puede ser relativamente posible; falsificar simultáneamente posición, tiempo, velocidad, dirección y coherencia Doppler sostenida es mucho más complejo. **[GNSS Spoofing Detection Based on Consistency Check of Velocities]()** y **[A GNSS Spoofing Detection Method Based on the Consistency of Measured and Calculated Carrier Dopplers]()** muestran precisamente que las inconsistencias entre Doppler, pseudorrangos, velocidad y dinámica del movimiento pueden delatar escenarios de spoofing aun cuando la solución de navegación aparente estabilidad superficial.

6.4 Alteraciones Doppler bajo jamming

El jamming afecta directamente la capacidad del receptor para mantener análisis Doppler estable, porque introduce ruido electromagnético suficiente para degradar el seguimiento limpio de las señales. Cuando esto ocurre, el receptor comienza a perder calidad de portadora, sincronización y continuidad de observación. El resultado no suele ser una narrativa falsa coherente, sino una degradación generalizada: inestabilidad de velocidad, pérdida abrupta de coherencia, ruido excesivo, caída de seguimiento satelital e interrupción de la navegación dinámica. En otras palabras, bajo jamming el sistema no “entiende” correctamente el entorno RF y deja de sostener una lectura física confiable del movimiento.
Desde el punto de vista táctico, una alteración Doppler por jamming suele expresarse como degradación inestable y pérdida de capacidad de validación, más que como una coherencia falsa bien construida. Esta diferencia es importante porque ayuda a distinguir entre negación de servicio y manipulación sofisticada. Cuando el Doppler se vuelve errático junto con la calidad de señal, la

hipótesis de interferencia por ruido gana fuerza; cuando la señal sigue pareciendo estable pero la dinámica física es incoherente, la sospecha puede orientarse más hacia spoofing que hacia jamming.

6.5 Alteraciones Doppler bajo spoofing

El spoofing representa un desafío mucho más sofisticado que el jamming porque la señal continúa existiendo y puede conservar apariencia de normalidad, pero su comportamiento físico ya no corresponde necesariamente a la realidad. Para engañar de forma convincente al receptor, un atacante no sólo debe alterar la posición visible, sino también sostener coherencia entre tiempo, velocidad, sincronización y dinámica Doppler. Esa exigencia técnica es una de las razones por las que el análisis Doppler resulta tan valioso: cuando el spoofing no reproduce correctamente la física del movimiento, pueden aparecer velocidades incompatibles, aceleraciones irreales, cambios bruscos o patrones imposibles respecto del trayecto mostrado.

En términos analíticos, la diferencia práctica es clara: el jamming tiende a producir pérdida, ruido y degradación; el spoofing tiende a producir aparente estabilidad con coherencia física imperfecta. **[GNSS Spoofing Detection Based on Consistency Check of Velocities]()** describe cómo la ruptura entre velocidad derivada de pseudorrangos y la información Doppler puede utilizarse como criterio de detección, mientras que **[Statistical Model and Performance Evaluation of a GNSS Spoofing Detection Method based on the Consistency of Doppler and Pseudorange Positioning Results]()** refuerza la idea de que la consistencia entre Doppler y posicionamiento es una vía sólida para identificar desvíos inducidos por spoofing.

6.6 El Doppler como herramienta de inteligencia operacional

El verdadero valor del Doppler no es únicamente técnico; es estratégico. Más allá del posicionamiento, permite analizar comportamiento, autenticidad, dinámica y coherencia operacional. Para una organización resiliente, esto significa que la seguridad ya no depende sólo de ver posiciones, sino de entender si el comportamiento físico observado tiene sentido real. En ese contexto, el Doppler puede convertirse en una herramienta de inteligencia operacional para detectar spoofing, validar rutas, identificar movimiento anómalo, confirmar autenticidad, mejorar detección temprana y reducir falsas interpretaciones.

Su mayor potencia emerge cuando se integra con INS, CAN Bus, telemetría, odómetro, acelerómetros y comportamiento geoespacial. Esa combinación permite construir confianza operacional no sobre la simple existencia de una coordenada, sino sobre coherencia, consistencia, autenticidad física y validación dinámica. El nuevo paradigma ya no pregunta solamente “¿tenemos GPS?”, sino “¿la información GNSS se comporta físicamente como debería?”. En operaciones modernas, la verdadera seguridad depende menos de recibir datos y más de comprender si esos datos reflejan una realidad auténtica. **[GNSS Spoofing Detection Based on Consistency Check of Velocities]()** y **[A GNSS Spoofing Detection Method Based on the Consistency of Measured and Calculated Carrier Dopplers]()** respaldan precisamente esta lógica de autenticidad basada en consistencia física y validación cruzada.

Módulo 7. Monitoreo inteligente y detección avanzada

Este módulo representa una transformación profunda en la forma de entender el monitoreo logístico y la seguridad operacional. Durante mucho tiempo, el monitoreo fue concebido como una actividad

esencialmente visual: observar un punto, confirmar una ubicación, revisar una alerta y reaccionar. Ese modelo fue funcional mientras las amenazas eran más visibles y la información disponible conservaba un grado razonable de confianza. Sin embargo, en el contexto actual, donde existen fenómenos capaces de degradar, negar o manipular la señal, ese enfoque resulta insuficiente. El problema moderno ya no consiste únicamente en saber dónde aparece una unidad en la plataforma, sino en determinar si la información observada es auténtica, coherente y utilizable para decidir.

El monitoreo inteligente parte de una premisa distinta: no basta con saber dónde está una unidad; es indispensable entender cómo se comporta, cómo se mueve, qué tan consistente es su narrativa digital y si sus distintas fuentes de información cuentan la misma historia. Esta diferencia cambia por completo la capacidad de detección. Un vehículo puede mostrar una posición aparentemente normal y, aun así, estar bajo interferencia, manipulación o alteración operativa que no se percibe a simple vista. Por ello, el monitoreo moderno debe integrar múltiples señales, comparar comportamientos, reconocer patrones y evaluar cuándo un dato parece estable, pero en realidad ya no merece confianza.

La detección avanzada no sustituye al GPS; lo complementa, lo cuestiona y lo valida dentro de un sistema más amplio de interpretación. Su objetivo no es generar más alertas, sino construir una confianza operacional mejor fundada. Esto exige pasar del seguimiento pasivo a la lectura integral del comportamiento, del punto aislado al contexto, y de la reacción automática a la interpretación inteligente. En términos prácticos, una organización madura no sólo observa datos: evalúa autenticidad, coherencia física, recurrencia, contexto geográfico, telemetría y patrones históricos antes de concluir qué está ocurriendo realmente.

Un vehículo puede mostrar una posición aparentemente normal y, aun así, estar bajo interferencia, manipulación o una alteración operativa que no se ve a simple vista. Por eso, el monitoreo moderno debe integrar múltiples fuentes de información, comparar comportamientos, identificar patrones y reconocer cuándo algo “sí parece funcionar”, pero en realidad no es confiable.

7.1 Más allá del punto en el mapa

El error más común del monitoreo tradicional es reducir toda la operación a una representación gráfica. La plataforma muestra un punto, una línea o una ruta, y surge la tentación de asumir que eso equivale a verdad. Sin embargo, el mapa no es la realidad; es la representación visual de datos recibidos y procesados. Por sí solo, no garantiza autenticidad, integridad ni coherencia. Monitorear inteligentemente significa ir más allá de la ubicación aparente y comenzar a observar comportamiento. Esto implica analizar si la unidad acelera o desacelera de forma lógica, si mantiene coherencia con la ruta asignada, si conserva continuidad entre eventos, si responde como debería responder físicamente y si la secuencia total de su actividad tiene sentido operativo. Un vehículo no sólo ocupa un lugar en el espacio: se mueve, se detiene, enciende, apaga, transmite, vibra y deja huellas de comportamiento. El monitoreo inteligente estudia precisamente esa totalidad.

Su importancia radica en que muchas amenazas no rompen el mapa de manera evidente; alteran la confianza en la información. Una posición puede ser falsa y parecer estable, una ruta puede verse limpia pero no coincidir con telemetría y un movimiento puede parecer normal en pantalla aunque sea físicamente imposible. Por ello, monitorear comportamiento es mucho más robusto que monitorear únicamente coordenadas.

7.2 Correlación multisensor

La correlación multisensor es una de las bases más importantes de la detección avanzada porque permite comparar lo que afirma una fuente con lo que reportan otras fuentes independientes. Si todas coinciden, aumenta la confianza; si se contradicen, aparece una señal de integridad comprometida. El GPS aporta posición, velocidad y tiempo, pero no debe considerarse infalible ni aislado. El INS estima movimiento a partir de acelerómetros y giroscopios y conserva valor incluso cuando el GNSS se degrada temporalmente. El CAN Bus permite leer variables internas del vehículo como velocidad, revoluciones, ignición, frenado o estado del motor. La red celular puede ofrecer una referencia territorial aproximada y validar cobertura o continuidad de comunicación. Los sensores físicos —como aperturas, temperatura, vibración o movimientos específicos— agregan evidencia sobre lo que realmente está ocurriendo en la unidad. La telemetría, por su parte, reúne información operativa del vehículo y del trayecto, y permite convertir un seguimiento simple en una lectura inteligente. La pregunta central de la correlación multisensor es muy simple y muy poderosa: ¿todas las fuentes cuentan la misma historia? Si el GPS dice una cosa, el CAN Bus otra y los sensores físicos otra distinta, el sistema ya no debe asumir normalidad. La verdadera detección comienza precisamente cuando las fuentes dejan de coincidir.
No ofrece la misma precisión que el GPS, pero puede ser útil para verificar:

7.3 Detección basada en patrones

La detección avanzada no se basa únicamente en alertas aisladas; se basa en reconocer patrones. Un patrón es una conducta que se repite de manera similar en el tiempo, en la geografía o en el comportamiento del evento. Cuando una anomalía se repite, deja de ser casualidad y comienza a convertirse en información útil para el análisis. Esto incluye corredores de riesgo donde históricamente se han presentado pérdidas de señal, desvíos, robos o interferencias; horarios en los que la vulnerabilidad aumenta por baja circulación, menor supervisión, cambio de turno o patrones criminales conocidos; tipologías de carga que elevan el interés delictivo por valor, facilidad de reventa o criticidad logística; y conductas recurrentes como pérdida GNSS en el mismo punto, caída de señal a la misma hora o coincidencia entre anomalías digitales y eventos físicos sospechosos. El valor del análisis de patrones radica en que aporta capacidad de anticipación. En lugar de reaccionar sólo cuando algo sucede, la organización aprende a reconocer dónde, cuándo, cómo y bajo qué condiciones aparece el riesgo. En ese momento, el monitoreo deja de ser una actividad pasiva y se convierte en una función real de inteligencia.
Hay ventanas en las que la vulnerabilidad aumenta por razones como:
Algunas presentan mayor exposición por:

7.4 Inteligencia geoespacial aplicada

La inteligencia geoespacial transforma los datos de ubicación en conocimiento estratégico. No se trata sólo de ubicar una unidad, sino de interpretar el territorio como un entorno de riesgo, oportunidad y comportamiento. Herramientas como mapas de calor permiten visualizar acumulaciones de pérdidas de señal, corredores con mayor incidencia, puntos con concentración de eventos sospechosos y áreas donde la operación se vuelve más frágil. Las geocercas dinámicas, a diferencia de las geocercas fijas, pueden adaptarse al comportamiento histórico, al nivel de riesgo, al tipo de carga, al horario y al contexto operacional, lo que permite una vigilancia más inteligente y

menos rígida. El análisis espacial, por su parte, ayuda a responder qué zonas comparten comportamiento similar, dónde aparecen anomalías repetidas, qué rutas concentran más incidentes y qué relación existe entre infraestructura, conectividad y riesgo. Esta dimensión geográfica es clave porque muchas amenazas no se entienden sin territorio. La interferencia GNSS, por ejemplo, puede guardar una relación estrecha con zonas urbanas densas, corredores carreteros específicos, patios logísticos, áreas industriales o tramos con historial de incidente. La inteligencia geoespacial convierte la ubicación en contexto y el territorio en una fuente activa de inteligencia operacional.

7.5 Inteligencia predictiva

La inteligencia predictiva busca adelantarse al evento y no sólo describirlo después. Su propósito es estimar la probabilidad de interferencia, degradación o comportamiento anómalo antes de que el impacto sea mayor. Para ello se apoya en variables como historial de incidentes, corredor utilizado, horario, tipo de carga, comportamiento reciente de la unidad, entorno físico y patrones operativos previos. Mientras más señales convergen, mayor será la probabilidad estimada de exposición. Sin embargo, el valor real de este enfoque no está únicamente en asignar un nivel de riesgo, sino en comprender que el riesgo es contextual y dinámico. Una misma ruta puede ser de bajo riesgo en un horario y de alto riesgo en otro; una misma unidad puede operar con estabilidad un día y volverse vulnerable al siguiente si cambian las condiciones operativas. La inteligencia predictiva permite pasar de una lógica reactiva a una lógica anticipatoria: en lugar de afirmar que ya ocurrió una pérdida de señal, el sistema comienza a advertir que existen condiciones suficientes para considerar que una unidad entra en una zona de riesgo elevado. Esa diferencia modifica por completo el nivel de preparación y la oportunidad de la respuesta.

7.6 Gestión de falsos positivos

Uno de los mayores retos del monitoreo avanzado es no confundir una anomalía real con un comportamiento normal del entorno. Un falso positivo ocurre cuando el sistema interpreta como amenaza algo que en realidad no lo es. Esto puede producir desgaste operativo, pérdida de confianza en la plataforma, saturación del monitoreo y respuestas innecesarias. Por eso, la gestión de falsos positivos es una parte esencial de la madurez operativa. Entre las causas más comunes se encuentran el drift natural del cálculo, el multipath urbano, la latencia celular y los errores de plataforma. El drift puede surgir por calidad del receptor, número de satélites visibles o condiciones normales del entorno. El multipath puede desplazar posiciones sin que exista interferencia intencional. La latencia celular puede alterar la secuencia aparente de eventos, y una mala lógica de software o una integración deficiente de datos puede generar desorden visible donde no existe amenaza real. La gestión madura de falsos positivos se apoya en tres principios: validar antes de escalar, correlacionar antes de concluir y observar contexto antes de activar una respuesta de crisis. La verdadera madurez no consiste en reaccionar a todo, sino en distinguir con criterio entre ruido, degradación normal y amenaza auténtica.
Puede ocurrir por:
El multipath es una fuente muy común de error que debe reconocerse para no sobrerreaccionar.

Cierre del módulo

El monitoreo inteligente deja atrás la lógica de observación pasiva y adopta una visión de análisis integral. Ya no basta con ver una ubicación; es necesario comprender comportamiento, correlación, contexto, territorio y consistencia física. La detección avanzada no busca únicamente encontrar alertas, sino construir confianza razonable en lo que se está observando. Cuando esa confianza no existe, el sistema debe ser capaz de reconocerlo antes de que la operación sufra el impacto. Esa es la diferencia entre un monitoreo meramente reactivo y una capacidad real de inteligencia operacional: no sólo registrar datos, sino interpretar con criterio cuándo esos datos siguen siendo útiles para decidir y cuándo han dejado de representar la realidad.

PARTE III — RESPONDER

La resiliencia operacional no se demuestra cuando todo funciona correctamente, sino cuando la organización es capaz de conservar control, coordinación, trazabilidad y capacidad de decisión aun bajo degradación tecnológica o incertidumbre operacional. Hasta este punto del manual se ha desarrollado una comprensión amplia sobre el funcionamiento del GNSS, sus vulnerabilidades, las amenazas que lo afectan y los métodos para detectarlas con mayor precisión. Sin embargo, comprender y detectar no son suficientes por sí mismos. El verdadero valor estratégico surge cuando la organización sabe cómo responder de manera estructurada en el momento en que la anomalía ya está ocurriendo.

La pregunta crítica de esta parte del documento es simple, pero decisiva: ¿qué debe hacer la organización cuando el evento ya está ocurriendo? Detectar una anomalía sin capacidad de respuesta coordinada no reduce realmente el riesgo. Una pérdida de GPS, una secuencia sospechosa de spoofing o una ruptura de trazabilidad pueden escalar rápidamente si el monitoreo, la seguridad, las operaciones, la inteligencia y el liderazgo no comparten criterios comunes para interpretar el evento y actuar con rapidez. Por ello, la respuesta moderna ante amenazas GNSS debe construirse sobre continuidad operativa, validación, escalamiento estructurado y preservación de información crítica. El objetivo no es únicamente recuperar señal; el objetivo es mantener control operacional aun cuando la información deje de ser completamente confiable.

Módulo 8. Respuesta táctica y continuidad operativa

La respuesta táctica frente a anomalías GNSS no puede depender de improvisación, intuición aislada o simples reflejos operativos. Requiere preparación previa, criterios claros de validación, mecanismos de escalamiento y capacidad para sostener la operación mientras se reduce la incertidumbre. En este módulo se aborda la respuesta no como una reacción impulsiva, sino como una disciplina organizacional orientada a preservar continuidad, proteger activos, mantener conciencia situacional y resguardar la información crítica que posteriormente permitirá auditar, investigar y aprender del evento.

La lógica de este módulo se organiza en tres tiempos complementarios: antes del evento, cuando la organización diseña prevención y prepara contingencia; durante el evento, cuando debe confirmar, contextualizar, coordinar y sostener control operacional; y después del evento, cuando transforma la experiencia en aprendizaje estructurado. Bajo esta perspectiva, responder no significa simplemente actuar rápido, sino actuar con fundamento, con proporcionalidad y con una arquitectura operativa capaz de seguir funcionando aun cuando la información principal se degrade parcial o temporalmente.

8.1 Qué hacer antes del evento

La respuesta efectiva comienza antes del incidente. Las organizaciones más resilientes no son necesariamente las que reaccionan más rápido, sino las que se preparan antes de que la degradación ocurra. La prevención reduce incertidumbre, improvisación, tiempo de reacción y vulnerabilidad operacional. En términos prácticos, esto significa que la operación no debe diseñarse únicamente en función de distancia, tiempo o costo. También debe considerar riesgo geoespacial, historial de incidentes, zonas de interferencia, infraestructura vulnerable, cobertura celular, exposición RF y nivel de criticidad operacional asociado a cada ruta, tipo de carga y ventana temporal.

La evaluación preventiva del riesgo no busca eliminar completamente la exposición, sino comprender dónde existe, cómo puede materializarse y qué impacto tendría sobre seguridad, continuidad y trazabilidad. Esta comprensión debe traducirse en planeación preventiva concreta: protocolos de contingencia, rutas alternas, validaciones secundarias, escalamiento predefinido, roles claros y canales redundantes de comunicación. La importancia estratégica de esta preparación radica en un principio fundamental: durante una crisis, las organizaciones no reaccionan según sus intenciones, sino según el nivel de preparación que construyeron previamente. Por ello, el diseño preventivo es ya, en sí mismo, una forma de respuesta táctica anticipada.

8.2 Qué hacer durante el evento

Cuando aparece una anomalía GNSS, el mayor riesgo inicial suele ser la incertidumbre. No siempre es evidente si se trata de degradación natural, falla técnica, interferencia, spoofing, sabotaje o evento criminal en curso. Por ello, la respuesta inicial debe enfocarse en confirmar, contextualizar y coordinar antes de concluir. La primera tarea no es asumir; es validar. Esto implica revisar si la anomalía es real, si es un evento aislado o recurrente, si existen otras fuentes afectadas, si la telemetría coincide, si hay coherencia multisensor y si el contexto geográfico o operativo ofrece una explicación plausible. Uno de los errores más comunes es escalar de inmediato cualquier pérdida GPS como ataque confirmado; esa reacción genera saturación, desgaste operativo y pérdida de credibilidad del monitoreo.

Una vez validado el nivel de riesgo, debe iniciarse un escalamiento estructurado, proporcional, contextual y coordinado. El objetivo es garantizar que seguridad, monitoreo, operaciones e inteligencia compartan la misma comprensión del evento y mantengan control operacional aun bajo incertidumbre parcial. La coordinación táctica puede implicar activar validación multisensor, incrementar supervisión, contactar operadores, verificar rutas alternas, revisar telemetría, correlacionar información externa y activar protocolos de contingencia. El principio fundamental es claro: durante un evento GNSS, la prioridad no es únicamente recuperar señal, sino preservar conciencia situacional y sostener capacidad de decisión mientras la organización determina qué está ocurriendo realmente.

8.3 Qué hacer después del evento

Uno de los errores más comunes es considerar que el incidente termina cuando reaparece el GPS, vuelve la comunicación o finaliza la anomalía visible. En realidad, ahí comienza el aprendizaje operacional. Toda anomalía significativa debe analizarse posteriormente con el mismo rigor con el que fue atendida durante la crisis. La investigación posterior debe reconstruir la línea temporal,

revisar comportamiento multisensor, evaluar persistencia del evento, ubicar el corredor geográfico, detectar patrones repetitivos, estimar el impacto operacional e identificar qué vulnerabilidades pudieron haber sido explotadas. El objetivo no es buscar únicamente culpables, sino comprender qué ocurrió, cómo ocurrió, por qué ocurrió y de qué manera puede reducirse la probabilidad de repetición.

Las organizaciones resilientes aprenden de cada evento. La retroalimentación posterior permite ajustar criterios, mejorar protocolos, redefinir alertas, actualizar mapas de riesgo, fortalecer el monitoreo y realizar ajustes operativos cuando sea necesario. Estos cambios pueden incluir modificación de rutas, ajustes tecnológicos, nuevas reglas de escalamiento, fortalecimiento multisensor, capacitación adicional y reconfiguración de alertas. La mejora continua es un principio central de la resiliencia: no se trata de alcanzar un estado permanente de seguridad perfecta, sino de adaptarse constantemente a un entorno donde las amenazas, las vulnerabilidades y las condiciones operativas cambian de forma continua.

8.4 Continuidad operacional bajo degradación GNSS

Uno de los conceptos más importantes de este manual es que la operación no debe detenerse automáticamente porque el GNSS se degrade. La continuidad operacional significa mantener capacidad de decisión, coordinación, supervisión y control razonable aun cuando exista incertidumbre parcial. La diferencia crítica entre una operación dependiente y una operación resiliente radica en esto: cuando falla el GNSS, la organización frágil pierde capacidad operativa; la organización resiliente activa validaciones alternas, protocolos, redundancias y mecanismos de continuidad que le permiten seguir funcionando sin quedar completamente ciega.

Entre los elementos clave de esta continuidad se encuentran la correlación multisensor, la comunicación redundante, los procedimientos de contingencia, el escalamiento estructurado, la inteligencia geoespacial y los protocolos adaptativos. El nuevo paradigma ya no consiste en evitar cualquier degradación, porque eso sería técnicamente irrealista; consiste en operar correctamente incluso bajo degradación parcial. En otras palabras, la meta no es construir operaciones imposibles de afectar, sino operaciones capaces de seguir gobernándose cuando la información principal pierde calidad o confiabilidad.

8.5 Preservación de trazabilidad crítica

La trazabilidad es uno de los activos más importantes en seguridad logística. Durante una anomalía GNSS, la información puede convertirse simultáneamente en evidencia, herramienta investigativa, soporte legal e insumo de inteligencia. Por ello, preservar trazabilidad crítica no es un aspecto secundario de la respuesta; es una prioridad operativa. Deben resguardarse logs, telemetría, eventos, secuencias temporales, registros multisensor, capturas de plataforma, historial de comunicación y correlaciones operativas relevantes. La razón es sencilla: después del evento, la organización necesitará reconstruir qué ocurrió, cuándo ocurrió y cómo evolucionó la anomalía para sostener auditoría, investigación, aprendizaje y validación posterior.

El riesgo crítico de no preservar trazabilidad durante la crisis es que la organización pierda la posibilidad de auditar, investigar y comprender con precisión el evento. En ese sentido, la información debe protegerse con el mismo nivel de prioridad con el que se protege la operación. Una organización madura reconoce que, en entornos GNSS degradados, cada dato confiable

preservado puede convertirse después en un elemento decisivo para interpretar el incidente, corregir vulnerabilidades y fortalecer la resiliencia futura.

Módulo 9. Matriz de respuesta logística y de seguridad

Las organizaciones resilientes necesitan algo más que tecnología: necesitan estructura de decisión. Una matriz de respuesta permite reducir improvisación, homologar criterios y coordinar áreas bajo un mismo lenguaje operacional. Su función no es burocratizar la reacción, sino garantizar que todos comprendan cuándo actuar, cómo actuar, quién debe actuar y bajo qué condiciones. En contextos donde la incertidumbre puede crecer rápidamente, esta claridad es un factor de control tan importante como la propia detección técnica.

La matriz de respuesta es, en esencia, un mecanismo de gobernanza operativa. Permite responder proporcionalmente al riesgo, evitar extremos de sobrerreacción o subestimación y asegurar que la decisión táctica se tome con criterios compartidos. En este módulo se desarrolla cómo clasificar niveles de alerta, definir criterios de activación, establecer roles y responsabilidades, estructurar el escalamiento, coordinar interáreas y activar protocolos de crisis cuando el evento supera la capacidad de respuesta normal.

Necesitan estructura de decisión.

Una matriz de respuesta permite:

- reducir improvisación,
- homologar criterios,
- y coordinar áreas bajo un mismo lenguaje operacional.

El objetivo no es burocratizar la reacción.

El objetivo es:

garantizar que todos comprendan:

- cuándo actuar,
- cómo actuar,
- quién debe actuar,
- y bajo qué condiciones.

9.1 Niveles de alerta

La clasificación por niveles de alerta permite responder proporcionalmente al riesgo. No toda anomalía requiere crisis máxima, pero tampoco toda degradación debe minimizarse. Una matriz madura distingue entre condiciones normales, incertidumbres iniciales, riesgos significativos y eventos críticos confirmados. El nivel verde corresponde a operación estable, señal coherente y riesgo controlado, donde basta el monitoreo rutinario. El nivel amarillo describe anomalías menores, degradaciones parciales o eventos no confirmados que requieren validación reforzada y observación más cercana. El nivel naranja aparece cuando existen múltiples indicadores correlacionados, comportamiento anómalo sostenido, posible interferencia deliberada o pérdida parcial de confianza operacional, lo que exige escalamiento táctico y activación de contingencia. El nivel rojo representa el escenario crítico: interferencia confirmada, pérdida severa de trazabilidad, riesgo criminal alto o compromiso operacional grave que obliga a activar protocolos de crisis. La utilidad estratégica de esta clasificación no está sólo en nombrar colores o estados, sino en construir criterios comunes de interpretación y respuesta. Cuando todos los equipos comprenden

qué significa cada nivel, se reduce la improvisación, se mejora la velocidad de decisión y se evita tanto el escalamiento tardío como la sobrerreacción frente a eventos todavía no confirmados.

9.2 Criterios de activación

Las alertas no deben activarse únicamente por la presencia de una anomalía; deben considerar contexto, persistencia, correlación e impacto operacional. Los criterios técnicos incluyen pérdida GNSS, inconsistencias Doppler, degradación multisensor, ruptura temporal y caída simultánea de sistemas. Los criterios operativos abarcan desvío de ruta, conducta anómala, pérdida de comunicación y eventos incompatibles con la operación normal. Los criterios contextuales, por su parte, incorporan corredores de riesgo, tipo de carga, historial geográfico, horario crítico e información de inteligencia disponible.

La fortaleza de una matriz de activación madura reside precisamente en combinar estos planos y no depender de un solo indicador. Una pérdida de GPS sin contexto puede ser un falso positivo; una pérdida de GPS asociada a ruta crítica, inconsistencia Doppler, telemetría contradictoria y patrón histórico similar constituye un escenario completamente distinto. Por ello, la activación debe ser el resultado de una evaluación estructurada y no de una respuesta automática a una sola señal.

9.3 Roles y responsabilidades

La resiliencia depende de claridad organizacional. El monitoreo es responsable de la observación, validación inicial, correlación de señales y escalamiento temprano. Seguridad asume la evaluación de amenaza, el análisis de riesgo, la coordinación táctica y la respuesta de protección. Operaciones sostiene la continuidad logística, el ajuste operativo, la coordinación de movimiento y el soporte al negocio. Inteligencia aporta análisis de patrones, correlación histórica, interpretación geoespacial y generación de contexto. Finalmente, el liderazgo es responsable de la toma estratégica de decisiones, la asignación de recursos, la coordinación ejecutiva y la continuidad organizacional.

La importancia de definir responsabilidades no radica sólo en repartir tareas, sino en evitar vacíos, duplicidades y contradicciones durante una crisis. Cuando cada área comprende su función y reconoce la función de las demás, la organización puede construir una respuesta integrada y sostenida. Sin esa claridad, el monitoreo puede saturarse, la seguridad puede sobredimensionar o subestimar la amenaza, operaciones puede perder continuidad y liderazgo puede recibir información fragmentada o inconsistente. La matriz de roles convierte esa complejidad en gobernanza operativa.

9.4 Escalamiento operativo

El escalamiento operativo debe ser progresivo, proporcional, documentado y coherente. Su finalidad es asegurar velocidad, claridad, coordinación y control operacional sin caer en extremos de reacción. Escalar demasiado tarde puede permitir que la amenaza se consolide; escalar todo como crisis máxima puede saturar a la organización, erosionar credibilidad y debilitar la capacidad de distinguir entre ruido y riesgo real. Por ello, un buen escalamiento no depende sólo de urgencia, sino de criterio.

El propósito del escalamiento es que la organización aumente capacidad de respuesta al mismo ritmo con el que aumenta la severidad del evento. Esto significa que cada transición de nivel debe activar recursos, validaciones, coordinación y liderazgo adecuados a la magnitud del incidente. De este modo, el escalamiento se convierte en un mecanismo de control y no sólo en una cadena de

avisos. Su valor estratégico reside en mantener la operación gobernable incluso cuando la incertidumbre aumenta.

9.5 Coordinación interáreas

Las amenazas GNSS afectan múltiples áreas simultáneamente, por lo que la respuesta aislada casi siempre resulta insuficiente. La coordinación interáreas requiere lenguaje común, intercambio de información, visión compartida, roles claros y objetivos alineados. Sin estos elementos, cada función interpreta el evento desde su propia lógica: monitoreo observa la anomalía técnica, operaciones se concentra en continuidad, seguridad evalúa amenaza y liderazgo dimensiona impacto. Si estas visiones no se integran, la organización corre el riesgo de responder con fragmentación, duplicidad o contradicción.

La coordinación interáreas convierte perspectivas distintas en una respuesta integrada. Su función estratégica es asegurar que toda la organización trabaje sobre una misma comprensión del evento, con criterios coherentes de validación, prioridad y acción. En operaciones resilientes, la coordinación no es un complemento administrativo; es una capacidad crítica de supervivencia organizacional frente a eventos ambiguos, veloces y técnicamente complejos.

9.6 Protocolos de crisis

Cuando la incertidumbre supera la capacidad operativa normal, la organización entra en modo crisis. En ese punto, ya no basta con observación reforzada o escalamiento táctico parcial; se requiere un protocolo de crisis capaz de mantener control, reducir incertidumbre, priorizar decisiones, preservar continuidad y proteger personas, activos e información. Los elementos fundamentales de ese protocolo incluyen comunicación clara, cadena de mando definida, validación continua, preservación de evidencia, coordinación multisistema y evaluación dinámica del riesgo. El objetivo es impedir que la crisis técnica se convierta en desorganización institucional.

La resiliencia operacional no significa evitar completamente la degradación. Significa mantener capacidad de comprender, decidir y actuar incluso cuando la información deja de ser perfecta. En operaciones modernas, la diferencia entre vulnerabilidad y resiliencia no está únicamente en la tecnología disponible, sino en la capacidad organizacional de responder inteligentemente bajo incertidumbre. Esa es la función central de la Parte III: traducir conocimiento técnico y capacidad de detección en estructuras concretas de respuesta, continuidad y gobernanza operativa.

PARTE IV — RESILIENCIA OPERACIONAL

La evolución de las amenazas GNSS obliga a sustituir una idea profundamente arraigada en muchas organizaciones: la seguridad no depende de tener tecnología perfecta, sino de sostener capacidad de operación aun cuando la tecnología presenta degradación, incertidumbre o manipulación. Durante años, numerosas operaciones logísticas fueron diseñadas bajo una lógica implícita: si existe señal GPS, existe control. Hoy esa premisa ya no es suficiente. La señal puede degradarse, la navegación puede manipularse y la información puede dejar de ser plenamente confiable sin que la operación lo detecte de inmediato.

Por ello, la resiliencia operacional no busca crear sistemas imposibles de afectar. Busca crear operaciones capaces de adaptarse, validar y continuar funcionando bajo condiciones adversas. Su lógica combina redundancia, validación multisensor, arquitectura híbrida, inteligencia contextual y

capacidad de decisión bajo incertidumbre. El objetivo final no es eliminar completamente el riesgo, sino evitar que una degradación tecnológica se transforme en pérdida de control operacional.

Módulo 10. Arquitectura resiliente y contramedidas

La resiliencia tecnológica no depende de una sola herramienta ni de un dispositivo excepcionalmente sofisticado. Depende de cómo se combinan múltiples capacidades para reducir puntos únicos de falla, sostener continuidad y preservar confianza operacional cuando la señal principal se degrada. En el contexto logístico, una arquitectura resiliente no es sinónimo de lujo tecnológico; es una necesidad estratégica para impedir que una afectación sobre GNSS se convierta automáticamente en pérdida de visibilidad, desorganización operativa o incapacidad de decisión. Este módulo desarrolla la resiliencia como una arquitectura de capas: fuentes múltiples de posicionamiento, bandas diversas, tecnologías complementarias de comunicación, navegación inercial, analítica distribuida, inteligencia artificial y procedimientos de redundancia tecnológica, operativa y humana. La lógica central es simple: si una capa falla, otras deben conservar capacidad suficiente para validar, sostener continuidad y permitir a la organización seguir gobernando la operación.

10.1 GPS vulnerable, operación resiliente

Uno de los errores estratégicos más graves es interpretar la vulnerabilidad tecnológica como sinónimo de inutilidad. No existe infraestructura completamente invulnerable: toda tecnología puede degradarse, fallar o verse afectada por el entorno. La madurez operacional no consiste en negar esa realidad, sino en prepararse para ella. Desde esta perspectiva, una operación resiliente no es la que nunca enfrenta fallas, sino la que puede mantener control razonable cuando las fallas ocurren. El cambio de paradigma es profundo: el enfoque tradicional intentaba evitar cualquier interrupción; el enfoque resiliente busca conservar capacidad operacional aun cuando existan degradaciones parciales, pérdida temporal de certeza o incertidumbre creciente.

La diferencia fundamental entre un modelo dependiente y un modelo resiliente es clara. En el primero, si el GPS falla, la operación pierde visibilidad, control y capacidad de decisión. En el segundo, la organización valida, correlaciona, activa redundancias y sostiene continuidad razonable mientras reduce incertidumbre. Por eso, la pregunta moderna ya no es si el GPS puede ser afectado; la respuesta es claramente sí. La verdadera pregunta es qué tan preparada está la organización para seguir operando correctamente cuando eso ocurra. La resiliencia implica adaptabilidad, tolerancia a la incertidumbre, continuidad y recuperación rápida; pero, sobre todo, implica aceptar que el GPS sigue siendo extraordinariamente útil sin tratarlo como única fuente absoluta de verdad, sino como parte de un ecosistema más amplio de validación operacional.

10.2 Arquitecturas resilientes

Una arquitectura resiliente no descansa en una sola constelación, una sola frecuencia ni un solo tipo de sensor. Se construye combinando múltiples capacidades que se complementan entre sí. La operación multi-constelación permite aprovechar sistemas como GPS, GLONASS, Galileo y BeiDou para incrementar disponibilidad, mejorar geometría satelital, reducir dependencia de una sola fuente y sostener navegación aun cuando una constelación presente degradación parcial. **[Multi-GNSS]()** y **[What is Multi-Constellation GNSS?]()** destacan precisamente que el

uso combinado de múltiples constelaciones incrementa la cantidad de satélites disponibles y fortalece continuidad, precisión y robustez.
La resiliencia mejora aún más cuando los receptores trabajan en múltiples bandas, ya que esto incrementa estabilidad, reduce parte de los errores atmosféricos y dificulta que una interferencia simple anule toda la capacidad de posicionamiento. A ello se suma la integración GNSS + INS, donde acelerómetros y giroscopios permiten mantener estimaciones de movimiento aun bajo degradación temporal del GNSS. El dead reckoning, por su parte, utiliza velocidad, dirección, historial de movimiento y comportamiento inercial para estimar continuidad de trayectoria durante periodos de pérdida parcial. Aunque estas técnicas acumulan incertidumbre con el tiempo y no sustituyen permanentemente al GNSS, sí son fundamentales para conservar continuidad temporal y reducir ceguera operacional en ventanas críticas. **[Dead Reckoning Navigation for UAS]()** y **[Fusing GNSS with Dead Reckoning: Accurate Navigation When Signals Drop]()** ilustran con claridad por qué la integración entre navegación satelital e inercial es un componente clave de resiliencia en entornos degradados.

10.3 Tecnologías complementarias

La resiliencia moderna no depende únicamente del GNSS. Depende de integrar tecnologías complementarias que permitan validar, comunicar, sostener redundancia y preservar continuidad cuando la fuente principal se degrada. La red celular, por ejemplo, puede funcionar como respaldo parcial para validar ubicación aproximada, mantener transmisión de eventos y sostener continuidad básica cuando el GNSS pierde precisión o disponibilidad. Esta lógica de fallback no significa sustituir completamente al posicionamiento satelital, sino contar con una tecnología secundaria capaz de aportar contexto y continuidad mientras la organización reduce incertidumbre.
Otras tecnologías complementarias amplían aún más la capacidad de continuidad. La comunicación satelital reduce el riesgo de aislamiento operacional cuando coinciden degradación GNSS y pérdida celular en zonas remotas o corredores críticos. Tecnologías como LoRa pueden sostener telemetría básica, sensores distribuidos o redes privadas ligeras con alta eficiencia energética. El edge analytics añade otra capa estratégica: permite procesar información directamente en el dispositivo o en el borde de la red, reduciendo latencia, detectando anomalías localmente y manteniendo funciones esenciales aun cuando la conectividad centralizada sea limitada. En conjunto, estas tecnologías no buscan reemplazar una plataforma principal, sino impedir que una sola afectación tecnológica desactive completamente la operación.

10.4 Detección basada en inteligencia artificial

El crecimiento del volumen de datos operativos vuelve cada vez más difícil depender exclusivamente de supervisión humana tradicional. La inteligencia artificial puede aumentar la capacidad de análisis al detectar correlaciones complejas, reconocer patrones recurrentes y señalar anomalías que resultarían difíciles de identificar manualmente dentro de grandes volúmenes de trayectorias, velocidades, eventos telemáticos, secuencias temporales y comportamientos geoespaciales. Su valor no radica en sustituir por completo al operador humano, sino en ampliar velocidad de detección, profundidad analítica y comprensión contextual.
No obstante, la inteligencia artificial no elimina automáticamente los falsos positivos ni convierte toda anomalía en amenaza real. Requiere entrenamiento adecuado, contexto operacional, datos de

calidad, validación cruzada y supervisión humana constante. En entornos GNSS complejos, una implementación madura de IA debe entenderse como inteligencia aumentada: la combinación entre experiencia humana, criterio operativo y capacidad computacional avanzada. Su función más valiosa es ayudar a que la organización reconozca comportamientos anómalos antes, con mayor consistencia y con mejor capacidad para priorizar lo verdaderamente relevante.

10.5 Estrategias de redundancia operacional

La redundancia es uno de los principios fundamentales de la resiliencia porque evita que un único punto crítico de falla destruya completamente la capacidad operacional. El error más común es construir operaciones basadas en una sola fuente GNSS, un solo canal de comunicación, una sola lógica de validación o una sola plataforma central. Esa dependencia crea fragilidad. Una estrategia madura distribuye la confianza entre múltiples constelaciones, múltiples bandas, sensores diversos y canales alternos de comunicación, de modo que una afectación parcial no se transforme automáticamente en ceguera total.

La redundancia no es sólo tecnológica; también es operativa y humana. Incluye rutas alternas, protocolos de contingencia, equipos de respaldo, validaciones secundarias, capacitación, criterio analítico y coordinación entre áreas capaces de sostener la gobernanza del evento. Su propósito no es eliminar todas las fallas, sino impedir que una sola falla paralice la operación. Ese es el núcleo de la resiliencia moderna: aceptar que existirán degradaciones, incertidumbres y amenazas, y construir sistemas capaces de adaptarse, validar, continuar operando y mantener control razonable aun cuando la realidad deje de ser perfecta. En seguridad logística contemporánea, la diferencia entre vulnerabilidad y resiliencia no está únicamente en tener más tecnología, sino en combinar arquitectura, inteligencia, redundancia y criterio para seguir funcionando bajo presión.

Módulo 11. Modelo de madurez operacional

Uno de los errores más frecuentes en seguridad logística consiste en asumir que todas las organizaciones enfrentan las amenazas GNSS con el mismo nivel de preparación sólo porque utilizan plataformas similares o dispositivos comparables. En realidad, dos empresas pueden operar con tecnología parecida y, aun así, tener capacidades completamente diferentes para detectar anomalías, validar información, coordinar áreas y responder bajo incertidumbre. La diferencia crítica no está únicamente en el hardware o en el software; está en el nivel de madurez operacional que la organización ha construido alrededor de esas herramientas.

La madurez operacional representa la capacidad de una organización para comprender riesgos, interpretar información de manera crítica, coordinar áreas, mantener continuidad bajo degradación tecnológica y transformar datos dispersos en decisiones útiles. Una operación madura no es aquella que nunca enfrenta incidentes, sino aquella que los detecta antes, los interpreta mejor, responde con menos improvisación y aprende sistemáticamente de ellos. Este modelo no busca etiquetar organizaciones como buenas o malas, sino ofrecer una estructura para entender dónde se encuentra actualmente la operación, cuáles son sus principales limitaciones y qué capacidades necesita desarrollar para evolucionar hacia niveles superiores de resiliencia.

11.1 Nivel 1 — Monitoreo reactivo

El nivel 1 corresponde al estado más básico de madurez operacional. En este punto, la organización depende casi por completo de la visualización GPS, de alertas simples y de la reacción posterior a eventos evidentes. El monitoreo está centrado en el mapa y asume implícitamente que, si existe una posición visible, existe control. La capacidad analítica es limitada: se revisa ubicación, se observa una ruta y se responde cuando aparece una pérdida de señal o una excepción claramente visible. El principal problema de este nivel no es la ausencia total de monitoreo, sino la falsa sensación de seguridad que produce ver movimiento en pantalla sin contar con validación contextual, correlación multisensor ni comprensión profunda de la amenaza. Las vulnerabilidades dominantes son alta dependencia del GNSS, respuesta tardía, escasa capacidad para detectar spoofing o manipulación y limitada comprensión del contexto operativo. La cultura organizacional predominante es reactiva y dependiente: la operación espera a que el problema se haga visible para comenzar a actuar.

11.2 Nivel 2 — Gestión por alertas

En el nivel 2 aparece una mejora importante: la organización deja de depender exclusivamente de observación manual y comienza a gestionar eventos mediante reglas automatizadas, alertas, geocercas y monitoreo por excepción. Este avance incrementa velocidad de reacción, orden operativo y trazabilidad básica de incidentes. Sin embargo, aunque existe más estructura, la lógica sigue siendo predominantemente reactiva. La operación responde mejor cuando una alerta se activa, pero todavía depende demasiado de eventos aislados, reglas rígidas y criterios poco contextuales. Un problema frecuente en este nivel es la saturación de alertas: cuando el sistema genera demasiadas notificaciones, aumenta la fatiga operativa, disminuye la atención real y se debilita la capacidad analítica. Por ello, el nivel 2 representa una evolución respecto del monitoreo puramente visual, pero aún no alcanza una comprensión madura del riesgo. La cultura operacional dominante puede describirse como reactiva estructurada: hay más disciplina y más automatización, pero todavía poca interpretación profunda.

11.3 Nivel 3 — Correlación multisensor

El nivel 3 marca uno de los cambios más relevantes en la madurez operacional: la organización deja de confiar en una sola fuente y comienza a comparar información entre múltiples sistemas. Aquí aparecen integración multisensor, validación cruzada, correlación entre GNSS, telemetría, CAN Bus y sensores físicos, así como una primera lectura contextual del evento. El cambio estratégico es decisivo: la pregunta deja de ser “¿tenemos señal?” y se convierte en “¿la información es coherente?”. Esta transición reduce falsos positivos, mejora la detección de anomalías y fortalece la capacidad de validar si una narrativa digital conserva autenticidad física. Aun así, el sistema sigue siendo principalmente reactivo: la organización comprende mejor el presente, pero todavía tiene capacidad limitada para anticipar el riesgo futuro. La cultura operacional en este nivel ya no es meramente reactiva; se vuelve analítica y correlacional, aunque aún no plenamente predictiva.

11.4 Nivel 4 — Inteligencia predictiva

En el nivel 4 la organización deja de limitarse a reaccionar y comienza a anticipar. Los modelos predictivos, el análisis histórico, la inteligencia geoespacial, la detección de patrones y la estimación de probabilidad de riesgo permiten reconocer condiciones previas a eventos críticos antes de que se materialicen plenamente. La operación ya no analiza sólo incidentes individuales; estudia

comportamiento, tendencias, recurrencias y contexto dinámico. Esto le permite identificar corredores de alto riesgo, horarios vulnerables, tipologías de carga especialmente expuestas y patrones compatibles con interferencia o actividad criminal. El beneficio principal de este nivel es que reduce tiempo de reacción, mejora asignación de recursos y convierte la inteligencia contextual en una herramienta preventiva. Sin embargo, aun aquí el riesgo nunca desaparece por completo: la inteligencia predictiva no elimina la incertidumbre, sólo la vuelve más comprensible y gestionable. La cultura operacional dominante en este nivel es anticipatoria e inteligente.

11.5 Nivel 5 — Resiliencia adaptativa

El nivel 5 representa la forma más alta de madurez operacional descrita en este modelo. En este punto, la organización ya no depende exclusivamente de una tecnología, de un proceso lineal o de una fuente única de verdad. La operación comprende que las degradaciones son inevitables y, por ello, diseña sistemas capaces de adaptarse dinámicamente bajo incertidumbre. Aquí convergen arquitectura resiliente, redundancia multisistema, continuidad operacional, validación contextual avanzada, inteligencia operacional integrada y capacidad real de coordinación interáreas madura. La diferencia fundamental de este nivel es que la organización no entra automáticamente en crisis cuando surge una degradación parcial; valida, adapta, prioriza y mantiene control razonable incluso cuando la información deja de ser perfecta. La cultura predominante es resiliente, adaptativa y estratégica: ya no se trata sólo de detectar o anticipar, sino de seguir gobernando la operación bajo presión y complejidad.

11.6 Evaluación de madurez organizacional

La madurez operacional no debe suponerse; debe evaluarse de manera explícita. Muchas organizaciones creen tener capacidades avanzadas simplemente porque cuentan con tecnología moderna, pero la verdadera madurez depende de integración, comprensión, procesos, coordinación y capacidad de decisión. Una evaluación seria debe observar al menos cuatro dimensiones complementarias. La primera es tecnológica: si existe redundancia, si se utilizan múltiples fuentes, si hay validación multisensor y si la arquitectura puede soportar degradación parcial. La segunda es de procesos: si los protocolos están definidos, si el escalamiento es claro, si existe continuidad operacional y si la trazabilidad se preserva adecuadamente. La tercera es humana: si el personal comprende las amenazas, recibe capacitación continua y entiende el contexto operacional. La cuarta es analítica: si la organización utiliza patrones, datos históricos, análisis geoespacial e inteligencia predictiva para interpretar el riesgo. En última instancia, la cultura organizacional es el reflejo más profundo de esta evaluación, porque la verdadera madurez depende de cómo la organización piensa y responde bajo incertidumbre, no sólo de las herramientas que posee.

11.7 Roadmap de evolución operativa

La evolución operacional no ocurre de manera instantánea; es un proceso progresivo que requiere claridad estratégica sobre el punto de partida y sobre las capacidades que deben desarrollarse. Un roadmap de evolución sirve precisamente para definir dónde se encuentra hoy la organización, qué brechas limitan su desempeño y cuál debería ser su secuencia lógica de fortalecimiento. En una fase inicial, la prioridad suele ser robustecer monitoreo, trazabilidad y control básico. En una fase intermedia, el foco se desplaza hacia correlación multisensor, validación contextual y análisis

operacional más consistente. En una fase avanzada, la organización incorpora inteligencia predictiva, automatización inteligente y arquitectura resiliente. Finalmente, en una fase madura, construye resiliencia adaptativa, continuidad operacional avanzada y capacidad de decisión bajo incertidumbre compleja. El principio central es que la madurez no consiste en tener más alertas, más plataformas o más datos, sino en transformar información en comprensión operacional útil. Las amenazas modernas no sólo ponen a prueba la tecnología; ponen a prueba la capacidad de análisis, la coordinación, la toma de decisiones y la resiliencia organizacional. La diferencia entre una operación vulnerable y una operación madura no está únicamente en los dispositivos que utiliza, sino en su capacidad para comprender el riesgo, validar la realidad, adaptarse bajo incertidumbre y mantener control operacional cuando las condiciones dejan de ser perfectas. En seguridad logística contemporánea, la verdadera ventaja estratégica no radica simplemente en ver más información, sino en comprender mejor lo que realmente está ocurriendo y actuar en consecuencia.

PARTE V — CRIMINOLOGÍA E INTELIGENCIA

Módulo 12. Criminología aplicada a interferencias GPS

Este módulo aborda las interferencias GNSS desde una perspectiva criminológica, es decir, no como fallas técnicas aisladas, sino como fenómenos que pueden integrarse dentro de secuencias delictivas planificadas. En seguridad logística moderna, el uso de jammers, spoofing, inhibidores celulares y mecanismos de ocultamiento digital no debe interpretarse únicamente como una curiosidad tecnológica. Debe entenderse como parte de una lógica criminal orientada a reducir visibilidad, retrasar reacción, fragmentar la trazabilidad y ampliar la ventana de oportunidad para el robo, el desvío o la desaparición de activos. La perspectiva criminológica es esencial porque permite vincular señales técnicas con conducta delictiva, territorialidad, temporalidad, oportunidad y profesionalización criminal.

La utilidad de esta lectura radica en que cambia la pregunta central de la organización. En lugar de preguntarse únicamente por qué falló la señal, la empresa comienza a preguntarse quién se beneficia de esa falla, qué ventana de oportunidad abre, qué patrón territorial acompaña al evento y cómo se relaciona con conductas previas, simultáneas o posteriores al robo. Bajo esta lógica, el jammer deja de ser sólo un dispositivo y se convierte en un facilitador criminógeno; el spoofing deja de ser sólo una manipulación técnica y se transforma en una herramienta de engaño operativo; y la pérdida de trazabilidad deja de ser únicamente un problema de monitoreo para convertirse en un factor que favorece impunidad, ocultamiento y debilitamiento de la capacidad institucional de respuesta.

12.1 El jammer como facilitador criminógeno

El jammer debe entenderse como un facilitador criminógeno porque incrementa la capacidad de éxito del delito sin reemplazar necesariamente la intervención física. Su valor para una célula criminal no está en destruir de forma permanente la tecnología de la víctima, sino en crear una ruptura temporal de supervisión suficiente para reducir capacidad de reacción, confundir al centro de monitoreo y aislar operativamente a la unidad. Esta condición altera el equilibrio entre empresa y agresor: mientras la organización pierde visibilidad, correlación y certeza situacional, el actor delictivo gana tiempo, margen de maniobra y menor exposición. Desde esta perspectiva, el jammer no es sólo un instrumento técnico, sino un multiplicador de oportunidad criminal.

Lo que vuelve criminógeno al jammer es precisamente su capacidad para transformar una operación supervisada en una operación vulnerable. Una unidad que deja de ser visible tarda más en ser localizada, pierde soporte táctico del centro de control, reduce la posibilidad de validación en tiempo real y se vuelve más fácil de mover, retener, transbordar o esconder. En términos criminológicos, esto significa que la interferencia no es el delito final, pero sí una condición facilitadora que disminuye resistencia institucional y aumenta la probabilidad de éxito del evento. Por eso, cuando una organización interpreta el jamming sólo como una falla técnica, subestima su verdadera relevancia como herramienta de preparación, ocultamiento y ejecución delictiva.

12.2 Conductas previas al robo

Antes del robo suele existir una fase de preparación que, desde criminología, debe analizarse como construcción de oportunidad. En esta etapa pueden aparecer conductas como reconocimiento de ruta, observación repetida de unidades, vigilancia discreta en puntos de parada, identificación de horarios vulnerables y búsqueda de información operativa interna. El objetivo de esa fase no es ejecutar todavía el delito, sino reducir incertidumbre, estudiar la respuesta de la empresa y preparar las condiciones para intervenir con menor exposición. Cuanto mayor conocimiento tenga el agresor sobre la carga, la ruta, las pausas, los tiempos y la reacción institucional, menor será su riesgo operativo.

Entre los indicadores previos más relevantes se encuentran seguimientos repetidos sobre una misma unidad o ruta, vehículos no identificados cerca de paradas recurrentes, consultas internas sospechosas sobre carga y custodia, cambios inusuales de horario sin justificación y pequeñas interrupciones de señal en tramos que más tarde presentan eventos mayores. La lectura criminológica de estos indicios es clara: la preparación delictiva busca convertir información dispersa en ventaja operativa. Por ello, la prevención no puede limitarse al blindaje del vehículo o al monitoreo en tránsito; también debe proteger la información crítica, la disciplina operativa y los patrones logísticos que podrían ser explotados por actores internos o externos.

12.3 Modus operandi contemporáneo

El modus operandi contemporáneo vinculado a interferencias GPS es más coordinado, adaptable y técnicamente asistido que el robo tradicional. Ya no depende exclusivamente de fuerza física o interceptación improvisada. En muchos casos, la secuencia delictiva comienza con selección de unidad o corredor, continúa con generación de ceguera temporal mediante interferencia o inhibición, pasa por el aislamiento operativo de la víctima y culmina con desvío, inmovilización, transbordo u ocultamiento posterior. Esta lógica secuencial es importante porque demuestra que la tecnología no aparece como elemento accesorio, sino como parte funcional del plan criminal. La interferencia digital puede preceder a la intervención física y, en ocasiones, determinar su viabilidad.

Desde criminología, lo más relevante no es sólo enumerar fases, sino comprender su efecto sobre la organización. Cada paso de la secuencia busca reducir el tiempo de reacción de la empresa y aumentar el control del agresor sobre el evento. La coordinación de grupos pequeños, el uso de vehículos de apoyo, la posible colusión interna y el uso de tecnología para aislar o engañar al monitoreo convierten el robo en una operación más racional y menos improvisada. Este cambio obliga a que la respuesta institucional también evolucione: ya no basta con reaccionar al asalto

físico; es necesario detectar con anticipación la preparación, la fase de ocultamiento y la ruptura de trazabilidad que suelen preceder o acompañar al delito.

12.4 Temporalidad y oportunidad criminal

La temporalidad es una variable central en la construcción de oportunidad criminal. Los grupos delictivos no suelen actuar al azar, sino en momentos donde la operación presenta menor capacidad de resistencia: cambios de turno, horarios nocturnos, madrugadas, periodos festivos, corredores con baja circulación o ventanas donde la supervisión es predeciblemente más débil. Desde criminología, esta selección temporal tiene una lógica simple: actuar cuando la reacción institucional será más lenta, cuando el apoyo será más limitado y cuando la percepción del evento podrá retrasarse algunos minutos críticos. En seguridad logística, esos minutos suelen marcar la diferencia entre un incidente contenido y un evento consolidado.

Por ello, la inteligencia debe correlacionar repetición de incidentes por hora, coincidencia entre turnos operativos y anomalías, picos de pérdida de señal en ventanas específicas y relación entre vulnerabilidad territorial y oportunidad temporal. El delito no ocurre solamente en un lugar; ocurre en un momento elegido. Esta comprensión permite pasar de una lectura estática del riesgo a una lectura dinámica donde territorio y tiempo se combinan para producir exposición criminal. Analizar horarios con el mismo rigor que se analizan rutas es, por tanto, una necesidad estratégica y no un detalle accesorio.

12.5 Ocultamiento digital y desaparición operativa

Después del robo o durante su ejecución, una de las prioridades criminales suele ser borrar, distorsionar o fragmentar la huella digital del evento. Este ocultamiento puede tomar varias formas: pérdida de señal, manipulación de la posición visible, reaparición artificial en otra ruta, trayectorias aparentemente normales o combinación de GNSS degradado con otras alteraciones telemáticas. El objetivo es impedir que la organización reconstruya con precisión lo ocurrido y, al mismo tiempo, generar confusión suficiente para retrasar decisiones críticas. Desde esta perspectiva, la desaparición operativa no debe entenderse sólo como ausencia de datos, sino como una estrategia deliberada de reducción de visibilidad y dilución de rastros.

La manifestación más peligrosa de este fenómeno es que puede mantener apariencia de normalidad superficial. Una unidad puede desaparecer y reaparecer, un trayecto puede parecer razonable, o una posición puede mantenerse estable sin resistir validación física. En estos casos, la organización corre el riesgo de auditar una narrativa falsa y tomar decisiones sobre una realidad digital alterada. La lectura de inteligencia es clara: el ocultamiento digital no busca únicamente esconder el activo, sino también confundir la interpretación institucional del evento, debilitar la investigación posterior y ampliar la impunidad operativa del agresor.

12.6 Correlación entre interferencia y eventos delictivos

La correlación entre interferencia y eventos delictivos es el punto donde el monitoreo técnico se transforma en inteligencia criminal. Cuando las pérdidas de señal, las caídas de comunicación o las anomalías de navegación se repiten en los mismos corredores, en horarios semejantes, con determinadas cargas o bajo patrones operativos parecidos, dejan de ser incidentes aislados y se convierten en indicios de un esquema delictivo recurrente. Esta correlación es esencial porque

permite vincular la anomalía tecnológica con el contexto criminal, reducir explicaciones simplistas y fortalecer la hipótesis de que la interferencia forma parte de una secuencia más amplia de preparación, ejecución u ocultamiento.
Las variables que deben correlacionarse incluyen fecha, hora, ubicación de la pérdida de señal, tipo de carga, ruta, tiempo de tránsito, intentos de robo, desaparición digital, alteraciones celulares y contradicciones multisensor. Cuando estas capas se superponen de manera consistente, la empresa puede dejar de ver la anomalía como "una falla" y empezar a tratarla como parte de un patrón delictivo. Ese paso es estratégico: permite anticipar riesgo, priorizar corredores, fortalecer protección de ciertas cargas y transformar observación reactiva en inteligencia preventiva.

12.7 Perfil operativo de células criminales

El perfil operativo de las células criminales vinculadas a robo al transporte e interferencia tecnológica suele caracterizarse por movilidad, coordinación, especialización funcional y aprovechamiento de información previa. No siempre se trata de grupos grandes; con frecuencia son células pequeñas, rápidas y adaptativas, capaces de combinar observación, uso de inhibidores, apoyo vehicular, armas, conocimiento de ruta y, en algunos casos, apoyo interno o filtración de información. Su fortaleza no está necesariamente en el volumen de integrantes, sino en la eficiencia con la que convierten información, oportunidad y tecnología en capacidad operativa.
Desde criminología, estos grupos deben entenderse como células adaptativas más que como estructuras rígidas. Coordinan por canales alternos, conocen rutas y tiempos de tránsito, identifican puntos débiles de supervisión y aprovechan ventanas de vulnerabilidad logística. Esa capacidad de adaptación explica por qué pueden operar con pocos integrantes y aun así generar alto impacto operacional. Para la empresa, reconocer este perfil es fundamental porque evita subestimar al adversario por tamaño y obliga a analizarlo por método, coordinación y capacidad de explotar debilidades sistémicas.

12.8 Inteligencia táctica aplicada al transporte

La inteligencia táctica aplicada al transporte convierte datos operativos en prevención concreta. Su finalidad no es únicamente explicar lo que ya ocurrió, sino reconocer señales tempranas para intervenir antes de que el daño sea mayor. Esto implica vigilar rutas de riesgo, patrones horarios, comportamiento multisensor, tipologías de carga, reportes previos de interferencia y cualquier indicio que permita inferir que una anomalía tecnológica forma parte de una secuencia delictiva en preparación o ejecución. La inteligencia táctica trabaja precisamente en ese umbral donde la información deja de ser descriptiva y comienza a convertirse en capacidad de anticipación.
En términos prácticos, esto exige mapear corredores con mayor incidencia, identificar horarios críticos, correlacionar pérdidas de señal con eventos delictivos, revisar posibles fugas internas de información y activar validación multisensor orientada a alerta temprana. El resultado esperado es que la empresa deje de operar a ciegas y construya una lectura del riesgo basada en patrones, no sólo en incidentes ya consumados. Cuando la inteligencia táctica funciona correctamente, la organización fortalece prevención, mejora respuesta y llega a las investigaciones posteriores con hipótesis más sólidas y menos dependientes de explicaciones improvisadas.

Cierre del módulo

La criminología aplicada a interferencias GPS permite comprender que el problema ya no pertenece exclusivamente al dominio técnico ni exclusivamente al dominio delictivo. Pertenece a ambos al mismo tiempo. Los jammers, el spoofing y otras formas de ocultamiento digital no son simples anomalías del entorno; son herramientas que pueden facilitar robo, reducir capacidad de reacción, debilitar trazabilidad y ampliar la impunidad operativa del agresor. La inteligencia táctica, por su parte, convierte esa comprensión en prevención, priorización y capacidad de anticipación. El valor estratégico de este módulo consiste precisamente en eso: ayudar a que la organización deje de interpretar las interferencias como eventos aislados y comience a leerlas como posibles componentes de una lógica criminal más amplia, organizada y adaptable.

Módulo 13. Inteligencia geoespacial y análisis de riesgo

Las amenazas modernas contra operaciones logísticas no ocurren de manera aleatoria ni se distribuyen de forma uniforme sobre el territorio. Tienden a concentrarse en determinados corredores, a repetirse bajo ciertas condiciones de horario, infraestructura y conectividad, y a manifestarse con mayor frecuencia allí donde convergen vulnerabilidad operativa, oportunidad criminal y debilidad de supervisión. Por ello, comprender el espacio geográfico ya no es únicamente una función de navegación; es una función de inteligencia estratégica. El territorio deja de ser un fondo pasivo del movimiento y se convierte en una variable activa que condiciona exposición, probabilidad de interferencia y capacidad de respuesta.

La inteligencia geoespacial permite transformar ubicaciones, trayectorias, anomalías y eventos en comprensión estratégica del riesgo. Su propósito no es sólo registrar dónde se encuentra una unidad, sino interpretar qué significa operativamente el entorno por el que transita, qué variables aumentan su exposición y qué patrones espaciales indican vulnerabilidad persistente. En operaciones modernas, el objetivo ya no es únicamente responder cuando ocurre un incidente, sino identificar dónde es más probable que ocurra, por qué ocurre en ese lugar y cómo reducir exposición antes de que la amenaza se materialice. Bajo esta lógica, el territorio ya no es únicamente un espacio físico: es un entorno dinámico de riesgo que debe ser leído, correlacionado y gestionado con el mismo rigor que la telemetría o la trazabilidad.

13.1 Corredores de riesgo

Un corredor de riesgo es una ruta, tramo o zona geográfica donde la probabilidad de interferencia, pérdida operacional, robo, sabotaje o degradación supera de manera consistente el promedio normal. Estos corredores existen porque ciertos territorios concentran vulnerabilidad física, baja supervisión, cobertura limitada, saturación urbana, historial de incidentes, infraestructura crítica deficiente o una combinación de oportunidad criminal y exposición logística. El riesgo rara vez está distribuido uniformemente: tiende a concentrarse en segmentos específicos donde confluyen fragilidad operativa y ventaja para el agresor. Uno de los errores más comunes es asumir que toda la ruta tiene el mismo nivel de amenaza. En la práctica, ciertos puntos acumulan pérdidas GNSS, eventos sospechosos y actividad criminal recurrente, mientras otros mantienen estabilidad relativa. Identificar estos corredores permite ajustar rutas, modificar horarios, reforzar monitoreo, aumentar validación multisensor y priorizar recursos de seguridad. La evolución estratégica consiste precisamente en dejar de analizar únicamente vehículos y comenzar a analizar territorios como sistemas de riesgo dinámico.

- interferencia,
- pérdida operacional,
- robo,
- sabotaje,
- o degradación,

es superior al promedio normal.

Analiza territorios.

13.2 Zonas RF hostiles

Una zona RF hostil es un entorno donde las condiciones de radiofrecuencia dificultan recepción, transmisión, validación o estabilidad operacional. No todas estas zonas son necesariamente criminales; algunas derivan de infraestructura compleja, saturación electromagnética, urbanización densa, túneles, parques industriales, zonas montañosas o áreas con alta contaminación RF. Otras, en cambio, pueden reflejar degradación deliberada. La diferencia entre una zona naturalmente degradada y una zona hostil intencional es crítica, porque una mala interpretación puede generar falsos positivos, respuestas incorrectas y pérdida de credibilidad operacional. Por ello, estas zonas deben analizarse con base en persistencia, intensidad, patrón geográfico, correlación multisensor, repetición histórica y compatibilidad contextual. Su importancia estratégica radica en que reducen visibilidad, estabilidad y capacidad de validación; en consecuencia, deben mapearse, monitorearse y contextualizarse de forma constante para que la organización pueda distinguir entre entorno complejo y señal de amenaza deliberada.

- recepción,
- transmisión,
- validación,
- o estabilidad operacional.
-

13.3 GEOINT aplicada a logística

La GEOINT, o inteligencia geoespacial, consiste en obtener comprensión operativa a partir de información geográfica y espacial. En logística moderna, esto significa interpretar comportamiento territorial, patrones de movimiento, zonas vulnerables, dinámicas operacionales e interacción entre infraestructura y riesgo. GEOINT no es simplemente “ver mapas”; es interpretar qué significa operativamente lo que ocurre en el territorio. Sus fuentes pueden incluir GNSS, telemetría, sensores, LTE, cartografía, eventos históricos, información criminal e infraestructura crítica. Lo valioso de este enfoque es que permite identificar corredores vulnerables, áreas de alta incidencia, conductas anómalas, patrones de degradación, zonas de oportunidad criminal y riesgo contextual dinámico. El cambio estratégico es profundo: la operación deja de preguntarse sólo dónde está el vehículo y comienza a preguntarse qué significa el entorno donde está operando. En ese sentido, GEOINT convierte datos espaciales en comprensión operacional y transforma el territorio en un activo analítico para prevención, anticipación y toma de decisiones.

13.4 Mapas de calor

Los mapas de calor permiten visualizar concentración de eventos dentro de un territorio y representan frecuencia, densidad o intensidad de actividad. En logística, su utilidad es amplia: pueden mostrar pérdidas GNSS, eventos de jamming, spoofing sospechoso, robos, desvíos, paros

anómalos o zonas de desconexión. Su ventaja radica en que el cerebro humano identifica patrones visuales con mucha mayor rapidez que grandes tablas de datos, lo que facilita detectar acumulaciones, visualizar recurrencias y priorizar zonas críticas. Sin embargo, su interpretación exige criterio. Un punto aislado no necesariamente representa una amenaza significativa, pero múltiples eventos concentrados pueden indicar vulnerabilidad estructural, corredor criminal o degradación recurrente. Al mismo tiempo, no toda concentración implica actividad delictiva; por ello, los mapas deben correlacionarse siempre con contexto, temporalidad, infraestructura y comportamiento multisensor. Bien utilizados, los mapas de calor permiten transformar datos dispersos en una lectura táctica del riesgo territorial.

13.5 Patrones territoriales

Los eventos logísticos rara vez son completamente aleatorios. Cuando se analizan suficientes datos, aparecen patrones territoriales: repeticiones consistentes de comportamientos, eventos, anomalías o riesgos asociados a un espacio específico. Estos patrones pueden manifestarse como pérdidas GNSS en el mismo tramo, incidentes recurrentes en determinados horarios, robos vinculados a zonas concretas, interferencia cerca de nodos logísticos o desconexiones repetidas en ciertas rutas. Su importancia estratégica radica en que permiten anticipar. Cuando una organización identifica frecuencia, recurrencia y coherencia entre eventos, deja de ver incidentes aislados y comienza a comprender dinámicas territoriales.

La utilidad táctica de esta lectura es profunda. Un patrón territorial no sólo describe dónde han ocurrido incidentes; ayuda a entender por qué tienden a ocurrir ahí, qué variables los favorecen y qué cambios pueden reducir exposición. Ignorar estos patrones suele provocar repetición de eventos, subestimación de amenazas y vulnerabilidad persistente, porque la organización continúa tratando cada incidente como si fuera independiente del anterior. En cambio, cuando los patrones se incorporan al análisis operativo, la empresa puede priorizar recursos, redefinir supervisión, ajustar rutas y convertir observación reactiva en inteligencia territorial aplicada a prevención.

Los eventos logísticos rara vez son completamente aleatorios. Cuando se analizan suficientes datos, aparecen patrones territoriales: repeticiones consistentes de comportamientos, eventos, anomalías o riesgos asociados a un espacio específico. Estos patrones pueden manifestarse como pérdidas GNSS en el mismo tramo, incidentes recurrentes en determinados horarios, robos vinculados a zonas concretas, interferencia cerca de nodos logísticos o desconexiones repetidas en ciertas rutas. Su importancia estratégica radica en que permiten anticipar. Cuando una organización identifica frecuencia, recurrencia y coherencia entre eventos, deja de ver incidentes aislados y comienza a comprender dinámicas territoriales. Ignorar estos patrones suele provocar repetición de incidentes, subestimación de amenazas y vulnerabilidad persistente. En cambio, reconocerlos permite priorizar recursos, modificar protocolos y transformar observación reactiva en conocimiento operativo sobre el territorio.

Y comienza a comprender:

dinámicas territoriales.

13.6 Riesgo dinámico operacional

El riesgo logístico no es estático. Cambia constantemente según territorio, horario, clima, tipo de carga, comportamiento operativo, cobertura RF y contexto criminal. Hablar de riesgo dinámico

significa reconocer que una ruta segura hoy puede no ser segura mañana, y que una operación estable en determinado momento puede volverse vulnerable si cambian las condiciones del entorno. Las organizaciones que trabajan con mapas de riesgo fijos tienden a tomar decisiones desactualizadas, pierden capacidad adaptativa y desarrollan una falsa sensación de seguridad. En contraste, una inteligencia geoespacial madura entiende que el riesgo debe actualizarse continuamente con base en variables de momento y no sólo en antecedentes históricos.
El objetivo de esta lógica dinámica es ajustar monitoreo, recursos, validación y respuesta según las condiciones reales del momento. El mismo evento puede representar baja amenaza en un entorno y alta amenaza en otro; por eso, el contexto es fundamental. La organización resiliente no sólo monitorea vehículos: monitorea territorio, comportamiento, contexto y evolución del riesgo. En ese sentido, la inteligencia geoespacial transforma el mapa en una herramienta de inteligencia operacional. Su valor no está únicamente en mostrar dónde se encuentra una unidad, sino en ayudar a comprender qué significa realmente el entorno donde está operando, qué riesgos la rodean y cómo anticiparse antes de que la amenaza se materialice.

PARTE VI — EVIDENCIA, AUDITORÍA Y GOBERNANZA

En seguridad logística moderna,
la información no sólo guía operaciones.
En operaciones modernas, la información ya no es únicamente soporte operativo. También puede convertirse en evidencia, elemento de auditoría, insumo de inteligencia, soporte de gobernanza y, en determinados contextos, base para procedimientos formales de investigación o reclamación. Cada evento GNSS deja huellas digitales: posiciones, trayectorias, alertas, telemetría, secuencias temporales y cambios de comportamiento que, correctamente preservados e interpretados, permiten reconstruir lo sucedido con un nivel de detalle crítico para comprender el incidente y mejorar la operación futura.
La diferencia entre una organización madura y una organización vulnerable no está solamente en detectar incidentes, sino en preservar correctamente la información, interpretar coherentemente los registros y garantizar integridad documental. Después de un evento crítico, la pregunta ya no es únicamente qué ocurrió, sino también cómo puede demostrarse, si la información es confiable, si la trazabilidad fue preservada y si la organización es capaz de reconstruir técnicamente la secuencia del incidente. En seguridad logística contemporánea, la evidencia operativa bien gestionada se convierte en memoria institucional; y sin memoria institucional, las vulnerabilidades tienden a repetirse.

Módulo 14. Evidencia digital y trazabilidad forense

14.1 GPS como evidencia

El GPS genera evidencia operativa de manera constante. Cada posición, trayectoria, velocidad, alerta, sello temporal o cambio de comportamiento registrado puede integrarse en una reconstrucción posterior del evento. Su valor evidencial proviene de que documenta movimiento, secuencia temporal, comportamiento logístico y relación entre la unidad y el territorio donde operó. En auditorías internas, investigaciones de incidentes, validación de rutas, soporte asegurador o reconstrucción de anomalías, la información GNSS suele constituir una de las primeras capas de

análisis disponibles. Sin embargo, su valor no depende únicamente de que exista un registro, sino de que ese registro conserve coherencia, integridad y contexto.
El error más peligroso en el manejo de evidencia GNSS consiste en asumir que, si el sistema lo muestra, necesariamente ocurrió exactamente así. El GPS no representa por sí mismo una verdad absoluta; representa una fuente técnica de información que debe validarse dentro de un contexto operacional más amplio. Su valor aumenta cuando existe coherencia multisensor, consistencia temporal, validación geográfica y adecuada preservación de registros. En consecuencia, la pregunta correcta no es sólo si existe evidencia GPS, sino si esa evidencia resiste una revisión crítica de autenticidad, continuidad y plausibilidad física.

¿Por qué el GPS tiene valor evidencial?
Representa:
una fuente de información técnica
que debe validarse dentro de un contexto operacional.

14.2 Integridad de registros

La integridad de registros significa que la información no fue alterada, corrompida, sobrescrita o manipulada después de su generación. En términos prácticos, una evidencia sin integridad pierde confiabilidad, valor analítico y credibilidad operativa. Los riesgos más comunes incluyen desincronización temporal, pérdida parcial de logs, cambios manuales no documentados, corrupción de archivos, fallas de almacenamiento y alteración deliberada. Por ello, no basta con conservar datos; es indispensable poder demostrar que esos datos permanecieron estables y protegidos desde su origen.
Desde una perspectiva madura, la organización debe poder responder con claridad cuándo se generó el dato, quién tuvo acceso, si fue modificado y cómo fue preservado. Esto exige sellos temporales confiables, sincronización adecuada, controles de acceso, historial de modificaciones y mecanismos de validación cruzada. La comprensión estratégica es simple pero decisiva: la información vale tanto como su confiabilidad. Si la organización no puede garantizar integridad, tampoco puede sostener con solidez auditoría, investigación o aprendizaje posterior.

¿Por qué es crítica?
La cadena de custodia digital documenta cómo fue preservada la información desde su generación hasta su análisis final. Su objetivo principal es garantizar que la evidencia permanezca íntegra, rastreable, verificable y defendible. Para ello, deben registrarse el origen de la información, fecha y hora, responsables de resguardo, accesos realizados, extracciones, transferencias, copias y procesos analíticos aplicados. Sin esta trazabilidad documental, aun una evidencia técnicamente valiosa puede perder credibilidad y fuerza analítica.
Un error frecuente consiste en preservar datos sin documentar quién los manipuló, cuándo lo hizo y bajo qué procedimiento. En entornos modernos, la cadena de custodia ya no puede limitarse a un solo archivo o a una plataforma aislada; debe considerar telemetría, servidores, registros celulares, sensores, eventos de plataforma y evidencia multisistema. La evidencia digital también requiere protección estructurada. Su valor futuro depende de la disciplina con que se conserve y documente durante todo el ciclo del incidente.

14.4 Preservación de logs

Los logs representan la memoria técnica de la operación. Documentan eventos, accesos, cambios, alertas, comportamiento del sistema y secuencias temporales que, después de un incidente, pueden ser decisivos para reconstruir lo sucedido. Su importancia radica precisamente en eso: permitir que la organización entienda no sólo qué ocurrió, sino también cómo evolucionó el evento y qué sistemas intervinieron. Los logs relevantes pueden incluir GNSS, telemetría, comunicación celular, sensores, eventos de plataforma, cambios de configuración y accesos administrativos.

En muchas investigaciones, el problema principal no es la ausencia total de información, sino que la información ya no existe o ya no conserva valor suficiente para análisis. Políticas cortas de retención, sobrescritura automática, mala administración, ausencia de respaldo o eliminación deliberada pueden destruir la capacidad de auditoría futura. Por ello, una estrategia seria de preservación debe definir tiempos de retención, niveles de criticidad, respaldo seguro, controles de acceso y mecanismos para impedir pérdida o alteración. La trazabilidad futura depende directamente de la preservación presente.

14.5 Correlación temporal

La correlación temporal consiste en reconstruir qué ocurrió, cuándo ocurrió y en qué secuencia ocurrió. Su importancia es crítica porque muchos eventos GNSS duran segundos, evolucionan rápidamente y afectan varios sistemas al mismo tiempo. Una línea temporal bien construida permite validar hipótesis, identificar incoherencias, distinguir causa y efecto y comprender si la anomalía corresponde a una degradación progresiva, a un ataque deliberado o a una combinación de factores. Para lograrlo, deben correlacionarse pérdida GNSS, comunicación celular, telemetría, movimiento físico, sensores, alertas y registros operativos.

Uno de los problemas más frecuentes es que sistemas distintos usan horarios diferentes, relojes desincronizados o sellos temporales inconsistentes, lo que dificulta auditoría, análisis forense y reconstrucción precisa del incidente. La precisión temporal puede definir si una hipótesis es coherente o no. Por ello, la sincronización de fuentes y la disciplina en los registros temporales no son un detalle técnico menor; son una condición estructural para sostener comprensión verificable del evento.

14.6 Validez operativa vs validez legal

No toda información útil operativamente posee automáticamente validez legal, y no toda información jurídicamente admisible basta por sí misma para comprender un evento operacional complejo. La validez operativa busca comprender y responder con rapidez, contexto y correlación. La validez legal, en cambio, busca demostrar formalmente con integridad, autenticidad, cadena de custodia y documentación verificable. Ambas dimensiones son necesarias, pero obedecen a lógicas distintas.

El riesgo organizacional aparece cuando se confunde evidencia operativa con evidencia jurídicamente sólida. Un dato puede ser muy útil para monitoreo y respuesta táctica, pero insuficiente para sostener un procedimiento formal si no conserva integridad documental. Por ello, una organización madura debe diseñar procesos capaces de sostener ambas dimensiones al mismo

tiempo: velocidad y contexto para decidir durante la operación, e integridad y trazabilidad para demostrar después lo ocurrido con suficiente robustez.

14.7 Auditoría de eventos GNSS

La auditoría de eventos GNSS busca evaluar qué ocurrió, cómo respondió la organización, qué funcionó y qué debe corregirse. No se limita a revisar si una alerta se activó; examina trazabilidad, integridad, respuesta operativa, correlación multisensor, tiempos de reacción, calidad de escalamiento y continuidad del negocio. La auditoría técnica revisa coherencia de datos y estabilidad de sistemas; la auditoría operativa examina decisiones, coordinación y cumplimiento de protocolos; y la auditoría estratégica analiza madurez organizacional, gestión de riesgo y resiliencia. Vista así, la auditoría no es una revisión administrativa, sino una herramienta de aprendizaje y fortalecimiento estructural.

En operaciones modernas, la información no sólo mueve la logística; también sostiene decisiones, investigaciones, auditorías, inteligencia y gobernanza organizacional. La verdadera fortaleza de una organización no está únicamente en generar datos, sino en preservar su integridad, garantizar trazabilidad, comprender contexto y convertir registros técnicos en conocimiento verificable. Cuando ocurre un incidente, la operación puede recuperarse; pero si la evidencia desaparece o pierde confiabilidad, la organización pierde comprensión, aprendizaje y memoria operacional. Y una organización sin memoria operacional tiende a repetir vulnerabilidades que ya habían aparecido antes.

El riesgo organizacional aparece cuando se confunde evidencia operativa con evidencia jurídicamente sólida. Un dato puede ser muy útil para monitoreo y respuesta táctica, pero insuficiente para sostener un procedimiento formal si no conserva integridad documental. Por ello, una organización madura debe diseñar procesos capaces de sostener ambas dimensiones al mismo tiempo: velocidad y contexto para decidir durante la operación, e integridad y trazabilidad para demostrar después lo ocurrido con suficiente robustez.

Referencias

Federal Aviation Administration. (2025). *Global Navigation Satellite System (GNSS) interference resource guide*. U.S. Department of Transportation. https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afx/afs400/afs410/GNSS

Lombardi, M. A., Narins, M., Enge, P., Peterson, B., Lo, S., Chen, Y.-H., & Akos, D. (2012). *The need for a robust, precise time and frequency alternative to GNSS*. GPS World.

Lombardi, M. A., Nelson, L. M., Novick, A. N., & Zhang, V. S. (2001). *Time and frequency measurements using the Global Positioning System (GPS)*. Cal Lab: The International Journal of Metrology.

McCarthy, J., Li-Baboud, Y., Brule, J., & Meldorf, K. (2023). *Foundational PNT profile: Applying the cybersecurity framework for the responsible use of positioning, navigation, and timing (PNT) services* (NISTIR 8323 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8323r1

National Institute of Standards and Technology. (2021). *Foundational PNT profile: Applying the Cybersecurity Framework for the responsible use of positioning, navigation, and timing services*

(NISTIR 8323). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8323

Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., & Capkun, S. (2011). *On the requirements for successful GPS spoofing attacks*. Proceedings of the 18th ACM Conference on Computer and Communications Security.

United States Department of Transportation. (2019). *National Positioning, Navigation, and Timing (PNT) Architecture*. U.S. Department of Transportation. https://www.transportation.gov/pnt/national-positioning-navigation-and-timing-pnt-architecture

United States Government. (2026). *Spectrum & interference issues*. GPS.gov. https://www.gps.gov/spectrum-interference-issues

United States Government. (2025). *GPS spectrum and interference issues*. GPS.gov. https://www.gps.gov/spectrum

United States Government. (2021). *Information about GPS jamming*. GPS.gov. https://archive.gps.gov/spectrum/jamming/

Warner, J. S., & Johnston, R. G. (2003). *GPS spoofing countermeasures* (Technical Report LAUR-03-6163). Los Alamos National Laboratory.

Yao, J., Weiss, M. A., Curry, C., & Levine, J. (2016). *GPS jamming and GPS carrier-phase time transfer*. Proceedings of the Precise Time and Time Interval Systems and Applications Meeting (PTTI).